Nineteen Hundred and Twenty-two

NYIPLA®

New York
Intellectual Property
Law Association

2022 NYIPLA Transactions Bootcamp
Day 2: October 12, 2022
Cybersecurity, IP, and Privacy Issues in Technology Transactions

- **Speakers:**
  - **Khalil Nobles**, Wilson Sonsini Goodrich & Rosati
  - **Nicole Spence**, IBM Corporation
  - **Jessica Turko**, Foley Hoag LLP
- **Moderator:**
  - **Diana Santos**, IBM Corporation

Agenda

- Cybersecurity Issues - Khalil Nobles
- Intellectual Property Issues – Nicole Spence
- Data Issues – Jessica Turko

Cybersecurity Issues

- What is cybersecurity?
- Cybersecurity vs information security
- Cybersecurity scenarios
- Drafting tips

What is Cybersecurity?

- Cybersecurity typically deals with protecting against the unauthorized electronic access to digital data.
- This typically includes protection against social engineering, phishing, phish kits, pretexting and baiting, all in an effort to access digital data.
- Cybersecurity has become an increasing focus in today's world. According to Norton, there is a cyberattack every **44 seconds throughout a day.**
- Cyberattacks may come from anywhere, but the U.S. is among the countries with the most cyber attackers.

Cybersecurity vs Information Security

- While cybersecurity and information security are often used interchangeably, there are technical differences between the two concepts.
- Cybersecurity aims to keep digital data secure, information security aims to keep data in **any form** secure.
- From a software licensing perspective, many customers do not have an understanding of the difference (nor do many vendors!), so contract discussions typically focus on the broader concept of information security instead of cybersecurity.

Challenging Cybersecurity Scenario(s)

- You are in-house counsel for a software vendor that hosts its SaaS software with a third-party provider. A prospective client has sent you its information security addendum as a condition to signing your software license. Your sales team has told you to do what it takes to get the agreement signed.
- You are in-house counsel for a software vendor that licenses sensitive data to financial services clients. One of your customers has conditioned its renewal of its agreement on you providing uncapped indemnification for current and future cybersecurity attacks and immediate notification of all such attacks. It would also like to permit its subsidiary in Iran to use your software.

Scenario(s) continued

- You are in-house counsel for a software company and a client would like to condition its renewal of its three-year agreement on a right to immediately terminate the agreement for any malware found your software.
- You are in-house counsel for a cybersecurity software company and are contracting with a government agency who will only sign the agreement if it is on the agency's form of vendor agreement. The vendor agreement contains provisions that you know that your company cannot comply with, but this is a key client for the company.

Drafting Tips

- As a licensee, try to use your company’s information security agreements instead of negotiating a vendor’s when possible.
- As a licensor, try to cap your indemnification obligations to amounts covered by your insurance policy (or lower).
- As either licensor or licensee, be sure to understand service level agreements, credits, confidentiality obligations and related terms, as the interplay between these concepts may lead to springing termination rights and obligations.
- As a licensor, avoid agreeing to information security related representations and warranties if you are unclear how they impact the agreement and your client’s obligations.
- As a licensor, a firm understanding of your licensee’s industry and regulatory pressures will help you to negotiate in a pragmatic fashion.

Intellectual Property Issues in Technology Transactions

- IP issues are present in all forms of agreements (e.g., employment agreements, merger agreements, NDAs). For technology transactions, the key is identifying IP issues for specific scenario.
- **Key IP Issues**:
  - Clearly defining and identifying the IP involved
  - Understanding the relationship of the parties
    - **Ownership**
    - Understanding the product to be developed and the services to be rendered
    - Understanding what your client wants from this relationship.

Intellectual Property Issues in Technology Transactions

- Terms/Scope of the License
- Escrow Provisions (esp. source code)
- Troubleshooting
  - Cure defects
  - Preventative Maintenance/Service Plans
- **Indemnification and Liability**

Challenging IP Scenarios

- **Independent Contractor/Development Agreements:** Where is the developer/independent contractor working from, and does the IP ownership and assignment rights fully cover the company under the laws of that country?
- **Merger Agreements:**
  - Does the IP definitions include all registered and unregistered IP?
  - What is the triggering event for any escrow provisions/agreements?
- **Software Agreements:**
  - Does the indemnification provision include IP infringement? Is there a cap for IP infringement?
  - Does the product include open-source? How is the open-source package linked? Is the open-source license permissive?
  - Are there any marketing or external public promotions related to the transaction? Any protocols or rules associated with the use of each parties' trademarks?
  - Is it clear who owns the product(s) (e.g., pre-existing vs. developed)?

Data Issues in Tech Transactions

- Several trends have converged to increase prominence of data issues in commercial contracts:
    - Increased enforcement penalties for data misuse: GDPR, CCPA have given teeth to data protection laws and forced companies to examine their data collection and protection practices.
    - IoT: more data is being collected from end users in more ways than ever before (cars, appliances, wearable devices); privacy challenges result.
    - AI / Machine learning: more clients rely on large data sets to "teach" their platforms how to process information. Challenge results from data being integrated into models.
- Commercial contracts have not kept up with this shift in prominence of data issues.
- Contracts often address data ownership, usage and privacy/disclosure rights inadequately, or in ways that may have unintended consequences.

Challenging Data Issues Scenarios

- Agreement does not even address data.
  - Agreement may have been drafted with focus on traditional categories of IP like patents and copyrights.
  - Data may be very important asset, but not adequately addressed in agreement.
  - Tip: Remember to review contracts with eye toward what's missing as well as what's included.
- Agreement does not distinguish between categories of data.
  - Data provided by each party
  - Data provided by third parties (customers, patients, etc.)
  - Data generated from the relationship
  - Ownership, use and disclosure rights may differ for each of these categories, and agreement may not capture these nuances.
  - Tip: Make sure you and your client have identified all types of, and concerns about, data.
- Your client and the counterparty both insist on owning data.
  - Does each party really need to own the data? Would a license be sufficient?
  - Co-ownership can be a quick fix but can create problems later
  - Tip: Educate your client on differences between ownership and license; is this your hill to die on?

Challenging Data Issues Scenarios

- Agreement addresses rights in data, but does not fully specify their scope
  - What is the duration of the right to use data? Does it survive termination or expiration of agreement?
  - Can the licensee sublicense rights to access and use the data? To whom? Can the licensee assign rights?
  - Territorial scope? Where will the data be processed?
  - Exclusive or non-exclusive? Are their field restrictions?
  - Tip: Remember again that what is missing can be as important as what is included. Develop checklists.
- Sweeping disclaimers and liability limitations have implications for data rights.
  - Beware of sweeping disclaimers re data and liability limitations related to "loss of data"
  - Tip: Carefully review laundry lists of excluded liabilities
- Supplemental documents may include important data provisions.
  - Beware of "contract creep" where supplemental documents include clauses with important implications for data issues
  - DPAs, Security Addenda are common places for data provisions to lurk
  - Tip: Make sure you understand how different documents work together in terms of precedence and control

Additional Resources

- https://us.norton.com/blog/emerging-threats/cybersecurity-statistics
- https://www.secureworks.com/blog/cybersecurity-vs-network-security-vs-information-security
- https://techjury.net/blog/how-many-cyber-attacks-per-day
- https://www.lexology.com/library/detail.aspx?g=a5c00798-c028-4225-87aa-1bc7ffbbd03a
- https://www.aipla.org/list/innovate-articles/incorporating-intellectual-property-rights-in-saas-agreements

Sample clauses:

- https://www.lawinsider.com/clause/cyber-security

Thank You

Questions?

iapp

Global Comprehensive Privacy Law Mapping Chart

Comprehensive data protection laws exist across the globe. While each law is different, there are many commonalities in terms of the rights, obligations and enforcement provisions. The Westin Research Center has created this chart mapping several comprehensive data protection laws, including the laws in the U.S., to assist our members in understanding how data protection is being approached around the world.

Our intent is to add to this chart and update it as laws are amended and other laws come into force. As always, we appreciate input from our members. If you have comments about the mapping or believe additional information should be included, please share it with Cathy Cosgrove at ccosgrove@iapp.org.

Special thanks to Perry Cruz, Amit Gadhia, Dr. Julien C. Hounkpe, Anna Johnston, Louisa Meliqsetyan, Selin Ozbek Cittone, Yechiel Steinmetz, Kezia Talbot, Daimhin Warner, and former IAPP legal externs, including Seth Azubuike, Brynne Duvall, Sean Kellogg, Eduardo Monteverde, and Cheryl Saniuk-Heinig, for their contributions.

Last updated: *April 2022*

Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

		Argentina	Armenia	Australia	Benin Republic
		Personal Data Protection Act*	Law On Personal Data Protection	Privacy Act 1988 Australian Privacy Principles (included in Privacy Act) Australian Privacy Principles Guidelines	Digital Code
INDIVIDUAL RIGHTS	Right to access	Articles 4(6) and 14	Articles 15, 18(1 and 4) and 20(1 and 2)	APP 12	Article 437
	Right to correct	Article 16	Articles 6, 15(2) and 21(2)	APP 13	Article 441
	Right to delete	Articles 4(5) and 16	Article 15(2)	APP Guidelines, APP 13 (related to correcting inaccuracy)	Articles 441, 443 and 444
	Right to portability				Article 438
	Right to opt out of all or specific processing		Articles 9(3), 11(2), 12(2) and 21(6)	APP 7	Articles 390 and 440
	Right to opt in for sensitive data processing	Articles 2 and 7*	Articles 12 and 13*	APP 3	Article 394
	Age-based opt-in right		Article 9(9)		Article 446
	Right not to be subject to fully automated decisions				Articles 401, 415 and 439
BUSINESS OBLIGATIONS	Notice/transparency requirements	Articles 6 and 13	Articles 9(5-8) and 10	APPs 1 and 5	Articles 384, 403, 415, 416 and 418
	Legal basis for processing		Article 8		Articles 383 and 389
	Purpose limitation	Article 4(3)	Articles 4(2), 16, 18(2) and 19(1)	APP 6	Articles 383(3) and 424
	Data minimization	Article 4(1), (7)	Articles 5, 18(2) and 19(1)	APP 3.1–3.2	Articles 383(4) and 424
	Security requirements	Article 9	Article 19 and Government Decision on Biometric Personal Data*	APP 11	Articles 383 and 426
	Privacy by design			APP Guidelines, APP 1, 1.3	Article 424
	Processor/service provider requirements	Article 9 (security)	Article 14		Article 386
	Prohibition on discrimination				Articles 393 and 401
	Record keeping	Chapter IV (Articles 21–28) (for data files, registers, banks, etc.)		APP Guidelines, APP 1, 1.5	Article 435
	Risk/impact assessments			Privacy Act 1988, 33D; APP Guidelines, APP 1, 1.7; Australian Government Agencies Privacy Code*	Article 428
	Data breach notification*		Article 21(3 and 4)	Privacy Act 1988, Part IIIC	Article 427
	Registration with authorities	Chapter IV (Articles 21–28) (for data files, registers, banks, etc.)	Article 23		Articles 405 and 406 (reporting obligation)
	Data protection officer			Australian Government Agencies Privacy Code*	Articles 430–432
	International data transfer restrictions	Article 12	Articles 26 and 27	APP 8	Articles 391 and 392
SCOPE	Exemption for employee data		Section 16 of Labour Code	Privacy Act 1988, 7B(3)	
	Nonprofits covered	Articles 1 and 2	Article 1(1)	Privacy Act 1988, 6C–6E OAIC guidance	Article 380
	Sectoral law carveouts		Article 1(2)		
	State-level preemption				
ENFORCEMENT	Independent enforcement authority	Agencia de Acceso a la Información Pública	Personal Data Protection Agency	Office of the Australian Information Commissioner	Autorité de Protection des Données à caractère Personnel
		Chapter V (Articles 29 and 30)	Articles 24 and 25	Privacy Act 1988, Part IV	Articles 462–490
	Rulemaking authority	Chapter V (Articles 29 and 30)	National Assembly, RA Government, Personal Data Protection Agency	Privacy Act 1988, 100	Article 483
	Fining authority	Article 31	Article 24; Article 189.17, Administrative Violations Code	Privacy Act 1988, Part III, 13G; Part IIIA; Part V, 46, 65–66, etc.	Articles 452-455, 459 and 483
	Criminal penalties	Articles 31 and 32	Article 145, Criminal Code (medical privacy)	Privacy Act 1988, Part V, 46, 65 and 66; Part VIA, 80Q, etc.	Articles 460 and 461
	Personal liability	Articles 31 and 32		Privacy Act 1988, 99A	Article 460
	Private right of action	Articles 33–39	Articles 17 and 21		Articles 449–451

***Data breach notification:** *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

***Argentina:** *Morrison Foerster's privacy library has an English version of the PDPA. The law provides no person can be compelled to provide sensitive data, subject to certain exceptions.*

***Armenia:** *The Law on Personal Data Protection has different categories of personal data, including "special category" personal data, "personal life data" and "biometric personal data." Armenia also has a decision regarding biometric personal data, RA Government Decision* N 1175-N *dated 15 October 2015 "On Defining Requirements for Material Carriers of Biometric Personal Data and Technologies for Storage of Such Data outside of Information Systems." The Armenian Constitution includes a right to privacy in Article 31.*

***Australia:** *The Australian Government Agencies Privacy Code requires Australian government agencies subject to the Privacy Act to conduct written privacy impact assessments for "high privacy risk" projects and requires the appointment of a privacy officer(s) and privacy champion.*

Global Comprehensive Privacy Law Mapping Chart

	Last updated: *April 2022* **Note:** *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*	**Brazil**	**Canada**	**China**	**Colombia**
		General Data Protection Law	Personal Information Protection and Electronic Documents Act	Personal Information Protection Law	Law 1581/2012* Law 1266/2008
INDIVIDUAL RIGHTS	Right to access	Articles 6(IV) and 18(II)	Schedule 1, Principle 9	Articles 44 and 45	Articles 8 and 18, Law 1581; Article 7, Law 1266; Article 21, Decree 1377
	Right to correct	Article 18(III)	Schedule 1, Principle 9	Article 46	Articles 8 and 18, Law 1581; Article 7, Law 1266; Article 22, Decree 1377
	Right to delete	Article 18(VI)	Schedule 1, Principle 9 (related to correcting inaccuracy)	Article 47	Articles 8 and 18, Law 1581; Article 7, Law 1266; Article 22, Decree 1377
	Right to portability	Article 18(V)		Article 45	
	Right to opt out of all or specific processing		Schedule 1, Principle 3 (4.3.8)	Articles 15 and 44	Article 8(e), Law 1581
	Right to opt in for sensitive data processing	Article 11	See OPC Guidance, Principle 3	Article 29	Articles 5 and 6, Law 1581; Article 6, Decree 1377
	Age-based opt-in right	Article 14		Article 31	Article 7, Law 1581*; Article 12, Decree 1377
	Right not to be subject to fully automated decisions	Article 20		Articles 24 and 55	
BUSINESS OBLIGATIONS	Notice/transparency requirements	Article 10, Section 2	Schedule 1, Principles 2, 3 and 8	Articles 7, 17, 23 and 30	Articles 4(e) and 12, Law 1581; Articles 14–18, Decree 1377
	Legal basis for processing	Article 7	Schedule 1, Principle 4.3 (consent required)	Article 13	Article 9, Law 1281; Article 5, Decree 1377 (consent based)
	Purpose limitation	Article 6(I)	Schedule 1, Principle 4	Article 6	Article 4(b), Law 1581
	Data minimization	Article 6(III)	Schedule 1, Principle 4	Articles 6 and 19	Articles 4 and 11, Decree 1377
	Security requirements	Articles 6(VII) and 46–49	Schedule 1, Principle 7	Articles 9, 51 and 59	Articles 4(g), 17 and 18, Law 1581; Article 19, Decree 1377
	Privacy by design				
	Processor/service provider requirements	Articles 37, 39 and 40		Article 21	Articles 8, 12, 17 and 18, Law 1581
	Prohibition on discrimination	Article 6(IX)		Article 16	
	Record keeping	Article 37	Part 1, Division 1.1, Section 10.3	Articles 54–56	Articles 8, 17 and 18, Law 1581; Articles 8 and 26, Decree 1377
	Risk/impact assessments	Article 38		Articles 55 and 56	Articles 17, 18 and 25, Law 1581
	Data breach notification*	Article 48	Part 1, Division 1.1, Sections 10.1–10.3	Article 57	Articles 17 and 18, Law 1581
	Registration with authorities			Articles 52 and 53	Article 25, Law 1581 (databases)
	Data protection officer	Article 41	Schedule 1, Principle 1	Article 52	Article 23, Decree 1377 (person or area designated to assume the function of personal data protection)
	International data transfer restrictions	Article 33		Articles 38–43	Article 26, Law 1581; Articles 24 and 25, Decree 1377
SCOPE	Exemption for employee data		Part 1, Section 4(1)(b)*		
	Nonprofits covered	Article 3	Part 1, Section 4	Article 3	Article 2, Law 1581
	Sectoral law carveouts				
	State-level preemption		See OPC Guidance		
ENFORCEMENT	Independent enforcement authority	National Data Protection Authority	Office of the Privacy Commissioner	*	Superintendency of Industry and Commerce
		Articles 55-A–55-L	Part 1, Division 2		Articles 19–24, Law 1581
	Rulemaking authority	Article 55-J	Part 1, Division 4, Section 26	Article 62	Article 21, Law 1581
	Fining authority	Articles 52–54	Part 1, Division 4, Section 28	Article 66	Articles 23 and 24, Law 1581; Title VII, Law 1266
	Criminal penalties			Article 71	
	Personal liability			Article 66	Articles 23 and 24, Law 1581; Articles 18 and 19, Law 1266
	Private right of action	Articles 42–45	Part 1, Division 2, Sections 14–17	Articles 50, 69 and 70	Article 16, Law 1266; Decree 2591

***Data breach notification:** *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

***Canada:** *PIPEDA applies to employee information in organizations engaged in federal works, undertakings or businesses.*

***China:** *Several government departments are responsible for enforcement, including the Cyberspace Administration of China, Ministry of Industry and Information Technology, and Ministry of Public Security.*

***Colombia:** *In addition to the data protection laws, there are decrees and other documents with relevant data protection provisions, including Decree 1377/2013 and Decree 2591/1991. Law 1581/2012 prohibits the processing of personal data of children and adolescents.*

Global Comprehensive Privacy Law Mapping Chart

Last updated: *April 2022*

Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

		European Union	Hong Kong	Israel	Kenya
		General Data Protection Regulation	Personal Data Privacy Ordinance*	Protection of Privacy Law	The Data Protection Act, 2019
			Data Protection Principles (PDPO Schedule 1)	Privacy Protection (Data Security) Regulations	The Data Protection Regulations, 2021*
INDIVIDUAL RIGHTS	Right to access	Article 15	Part 5, Division 1, Section 18; DPP 6	Article 13	Section 26(b)
	Right to correct	Article 16	Part 5, Division 2, Section 22	Article 14	Sections 26(d) and 40
	Right to delete	Article 17	DPP 2 (related to correcting inaccuracy)	Articles 14 (related to correcting inaccuracy) and 17F(b) (direct mailing)	Section 26(e) (if false or misleading data) and 40 (limited)
	Right to portability	Article 20			Section 38
	Right to opt out of all or specific processing	Articles 7 and 21	Part 6A, Division 2, Section 35G		Sections 26(c), 32, 34 and 36
	Right to opt in for sensitive data processing	Article 9			*
	Age-based opt-in right	Article 8			Section 33
	Right not to be subject to fully automated decisions	Article 22			Section 35
BUSINESS OBLIGATIONS	Notice/transparency requirements	Article 12	DPPs 5 and 6	Article 11	Sections 25(b), (e) and 29
	Legal basis for processing	Article 6	DPP 1	Article 1	Section 30
	Purpose limitation	Article 5(1)(b)	DPPs 1 and 3	Articles 2(9) and 8(b)	Section 25(c)
	Data minimization	Article 5(1)(c)	DPP 1	Article 2(c), Privacy Protection (Data Security) Regulations*	Sections 25(d) and 39
	Security requirements	Article 32	DPP 4	Articles 17 and 17B; Privacy Protection (Data Security) Regulations	Sections 19(2)(e), 29(f), 41 and 42
	Privacy by design	Article 25			Section 41
	Processor/service provider requirements	Article 28	DPPs 2(3) and 4(2)	Articles 17 and 17A; Articles 15 and 19, Privacy Protection (Data Security) Regulations	Parts III and IV; Part IV, General Regulations
	Prohibition on discrimination	Recital 71			
	Record keeping	Article 30	Part 5, Division 3, Section 27	Articles 6(b), 10, 11, 15(a)(2)(d), 17, 18, and 19, Privacy Protection (Data Security) Regulations	Section 43(8) (data breach); General Regulation 19
	Risk/impact assessments	Article 35		Article 5(c), Privacy Protection (Data Security) Regulations	Section 31; Part VIII, General Regulations
	Data breach notification*	Article 33 Article 34		Article 11(d), Privacy Protection (Data Security) Regulations	Section 43; Part VI, General Regulations
	Registration with authorities	Article 37(7)	Part 4, Section 15	Article 8(a)(1) (databases)	Sections 18-22; Registration of Data Controllers and Data Processors Regulations
	Data protection officer	Article 37		Article 17B (security supervisor)*	Section 24 (optional)
	International data transfer restrictions	Articles 44–50	Part 6, Section 33 (not yet in operation)	Privacy Protection (Transfer of Data to Databases Abroad) Regulations	Sections 25(h) and Part VI; Part VII, General Regulations
SCOPE	Exemption for employee data		Part 8, Sections 53 and 54		
	Nonprofits covered	Article 2	Part 1, Section 2	Article 1; Article 4 of the Interpretation Law	Section 4
	Sectoral law carveouts	Article 6(2)		Article 13(c)(3)	
	State-level preemption	Recital 10			
ENFORCEMENT	Independent enforcement authority	EU national data protection authorities	Office of the Privacy Commissioner for Personal Data	Privacy Protection Authority	Office of the Data Protection Commissioner
		Articles 51–59	Part 2, Section 5	Articles 9, 10, 10A, and 12 (database registration); Articles 11(d) and 20, Privacy Protection (Data Security) Regulations	Sections 5-17
	Rulemaking authority	Articles 64, 65(1)(c) and 92	Part 3, Section 12	Article 36; the Privacy Protection Authority	Sections 5, 8, 9 and 74
	Fining authority	Article 83	Part 7, Sections 35C, 50A, 64, etc.	Privacy Protection Authority	Sections 9(1)(f) and 63
	Criminal penalties		Numerous provisions	Articles 5, 6, 16, 29A, 30, 31A and 31	Section 73
	Personal liability		Director convicted under PDPO	Articles 4, 17, 17B(b), 30, 31A, 31B and 31	
	Private right of action	Article 79	Part 9, Section 66	Articles 4, 15, 17F(e), 30, 31B and 31	Section 65

***Data breach notification:** *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

***Hong Kong:** *The Personal Data (Privacy) (Amendment) Ordinance 2021 focused on combating doxxing acts took effect Oct. 8, 2021.*

***Israel:** *As with most countries, there are other laws in Israel that may be relevant to data privacy, including the Basic Law: Human Dignity and Liberty that provides all persons the right to privacy (Article 7) and Communications Law (Bezeq and Transmissions) (Amendment No. 72), 2018. The PPA has publications on topics like data minimization, cross-border transfers and the appointment of data protection officers.*

***Kenya:** *The Data Protection Regulations include general regulations, regulations regarding complaints handling and enforcement procedures, and regulations regarding registration of data controllers and data processors. Kenya limits the grounds for processing sensitive personal data (Sections 44 and 45) and personal data relating to the health of a data subject (Section 46).*

iapp

Global Comprehensive Privacy Law Mapping Chart

Last updated: *April 2022*

Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

		New Zealand	Nigeria	Philippines	Singapore
		Privacy Act 2020 Information Privacy Principles (Part 3, Subpart 1 of the Privacy Act) Codes of practice	Nigeria Data Protection Regulation Nigeria Data Protection Regulation Implementation Framework	Data Privacy Act of 2012 (R.A. 10173)* Implementing Rules and Regulations of the Data Privacy Act of 2012	Personal Data Protection Act
INDIVIDUAL RIGHTS	Right to access	IPP 6; Part 4, Subpart 1	Paragraph 3.1 (6) and (14)	Section 16(c); IRR, Rule VIII, Section 34(c)	Section 21
	Right to correct	IPP 7; Part 4, Subpart 2	Paragraph 3.1(7)(h)	Section 16(d); IRR, Rule VIII, Section 34(d)	Section 22
	Right to delete	IPP 7; Section 7(1); Part 4, Subpart 2 (related to correcting inaccuracy)	Paragraph 3.1(9)	Section 16(e); IRR, Rule VIII, Section 34(e) (certain circumstances)	Section 25 (obligation limiting retention)
	Right to portability		Paragraph 3.1(14) and (15)	Section 18; IRR, Rule VIII, Section 36	Sections 26F–26J*
	Right to opt out of all or specific processing		Paragraphs 2.3(c) and 3.1(11)	IRR, Rule VIII, Section 34(b)	Section 16
	Right to opt in for sensitive data processing		NDPR Framework, Articles 5.3.2 and 5.4*	Section 13; IRR, Rule V, Section 22	
	Age-based opt-in right		NDPR Framework, Articles 5.3.1(d), 5.4 and 5.5*	*	*
	Right not to be subject to fully automated decisions		Paragraph 3.1(7)(L); NDPR Framework, Articles 3.2 (xvi) and 5.3.1(f)	Section 16(c)(6); IRR, Rule VIII, Section 34(b)	
BUSINESS OBLIGATIONS	Notice/transparency requirements	IPP 3	Paragraphs 2.5, 3.1(1) and (7); NDPR Framework, Annex B (Privacy Policy Template)	Sections 11 and 16(a) and (b); IRR, Rule IV, Section 18(a) and Rule VIII, Section 34(a)	Sections 12(d) and 20
	Legal basis for processing	IPPs 10 and 11 (post-collection)	Paragraph 2.2	Section 12; IRR, Rule V	Section 13 (consent required)
	Purpose limitation	IPP 10	Paragraphs 2.1(1)(a) and 3.1(7)(m); NDPR Framework, Article 4.1	Sections 11 and 12; IRR, Rule IV, Sections 18 and 19.	Sections 18 and 20
	Data minimization	IPPs 1 and 9 (storage limitation)	NDPR Framework, Annex A (Audit Template), No. 4.6	Sections 11(d) and (e); IRR, Rule IV, Section 19(d) and Rule VI, Section 26(e)	Section 14(2)(a)
	Security requirements	IPP 5	Paragraphs 2.1(1)(d) and 2.6; NDPR Framework, Article 3.2(v)	Chapters V and VII; IRR, Rules VI and VII	Section 24
	Privacy by design				
	Processor/service provider requirements	IPP 5; Section 11	Paragraph 2.7; NDPR Framework, Article 3.2	Sections 14, 20(d) and 21; IRR, Rule VI, Section 26(f) and Rule X	Section 4(2)
	Prohibition on discrimination				
	Record keeping		NDPR Framework, Annex A (Audit Template), No. 3.1	IRR, Rule VI, Section 26(c)	Section 22A
	Risk/impact assessments		Paragraph 4.1(5)-(7) (audit requirement); NDPR Framework, Articles 3.2(viii) and 4.2 (data protection impact assessment)	Section 20(c); IRR, Rule VI, Section 29; NPC Advisory No. 2017-03, Guidelines on Privacy Impact Assessments	*
	Data breach notification*	Part 6, Subpart 1	NDPR Framework, Articles 3.2(ix) and 9	Section 20(f); IRR, Rule IX	Sections 26A–26E
	Registration with authorities			IRR, Rule XI; NPC Circular 17-01	Section 11(5)*
	Data protection officer	Section 201	Paragraph 4.1(2); NDPR Article 3.4-3.7	Section 21(b); IRR, Rule VI, Section 26(a) and Rule XII, Section 50(b)	Section 11
	International data transfer restrictions	IPP 12; Part 8	Paragraphs 2.11-12 and 3.1(8); NDPR Framework, Articles 7 and 14	Section 21; IRR, Rule XII	Section 26
SCOPE	Exemption for employee data			Section 4 (limited to government officers, employees and contractors)	First Schedule, Part 3 Legitimate Interests, Section 10
	Nonprofits covered	Section 8	Paragraph 1.2; NDPR Framework, Article 2.1	Section 4	Section 4
	Sectoral law carveouts	Sections 24 and 28		Section 4	Section 4(6)(b)
	State-level preemption				
ENFORCEMENT	Independent enforcement authority	Office of the Privacy Commissioner	Nigeria Data Protection Bureau*	National Privacy Commission	Personal Data Protection Commission
		Part 2	Paragraph 4.2; NDPR Framework, Article 10	Chapter II; IRR, Rule III	Sections 5–10
	Rulemaking authority	Part 3, Subpart 2	Preamble to NDPR	Chapter II; IRR, Rule III	Section 65
	Fining authority		Paragraph 2.10; NDPR Framework, Article 10.1.4	Sections 7(i); IRR, Rule III, Section 9(f)	Sections 48C–48F, 48J–48K, 51–52A and 56
	Criminal penalties	Sections 104, 118, 197 and 212	Paragraph 2.10; NDPR Framework, Article 10.1.5	Chapter VIII; IRR, Rule XII, Section 51 and Rule XIII	Sections 48C–48F, 51–52A and 56
	Personal liability	Sections 12, 27, 119, 120, and 211		Chapter VIII; IRR, Rule XII, Section 51 and Rule XIII	Sections 48C–48F, 48J–48K, 51–52A, 56 and 60
	Private right of action	Section 31		Section 16(f); IRR, Rule VIII, Section 34(f) and Rule XII, Section 51	Section 48O

***Data breach notification:** *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

***Nigeria:** *Explicit consent is required for the processing of sensitive personal data. Consent is required for the processing of the personal data of a minor. A child is defined as any person under 13. The National Information Technology Development Agency issued the NDPR and was the main regulator. In February 2022, the government of Nigeria created the NDPB to oversee implementation of the NDPR.*

***Philippines:** *The NPC has issued a number of guidance documents regarding the interpretation of the DPA and the IRR that may be informative. For example, in Advisory Opinion* No. 2017-49, *the NPC stated "a minor cannot validly provide the consent as defined under the DPA."*

***Singapore:** *Amendments to the PDPA not yet in effect will create a right of portability and increase potential financial penalties. The PDPC has issued Advisory Guidelines on various topics, including data activities related to minors and data protection impact assessments. There is no DPO registration requirement but the law does require DPO contact details be made public.*

Global Comprehensive Privacy Law Mapping Chart

Last updated: *April 2022*

Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

		South Africa	South Korea	Turkey
		Protection of Personal Information Act Regulations Relating to the Protection of Personal Information	Personal Information Protection Act	Law on the Protection of Personal Data
INDIVIDUAL RIGHTS	Right to access	Sections 5(b), 23 and 25*	Articles 4 and 35	Chapter 3, Article 11
	Right to correct	Sections 5(c) and 24; Regulation 3	Articles 4 and 36	Chapter 3, Article 11
	Right to delete	Sections 5(c) and 24; Regulation 3	Articles 4 and 36	Chapter 2, Article 7; Chapter 3, Article 11 (limited)
	Right to portability			
	Right to opt out of all or specific processing	Sections 5(d)-(e) and 11(3)-(4)	Articles 4 and 37	
	Right to opt in for sensitive data processing	Sections 26–33 (“special personal information”)	Article 23	Chapter 2, Article 6
	Age-based opt-in right	Sections 34 and 35	Article 22(6)	
	Right not to be subject to fully automated decisions	Sections 5(g) and 71		Chapter 3, Article 11(1)(g)
BUSINESS OBLIGATIONS	Notice/transparency requirements	Sections 5(a) and 18	Articles 3, 4 and 30	Chapter 3, Article 10(1)
	Legal basis for processing	Sections 4, 9 and 11	Articles 3 and 15	Chapter 2, Articles 4–6
	Purpose limitation	Sections 13 and 15	Articles 3, 15, 18 and 19	Chapter 2, Article 4(2)(c)
	Data minimization	Sections 10, 14 and 16	Article 16(1)	Chapter 2, Article 4(2)(ç) and (d)
	Security requirements	Sections 19–21	Article 29	Chapter 3, Article 12
	Privacy by design			
	Processor/service provider requirements	Sections 20 and 21 (security)	Articles 19 and 26	Chapter 3, Article 12
	Prohibition on discrimination			
	Record keeping	Sections 14 and 17	Article 29	Chapter 4, Article 16
	Risk/impact assessments	Regulation 4(b)	Article 33	
	Data breach notification*	Section 22	Article 34	Chapter 3, Article 12(5)
	Registration with authorities	Sections 55 (for Information Officers) and 58 (certain processing); Guidance Note on Application for Prior Authorisation*	Article 32	Chapter 4, Article 16
	Data protection officer	Sections 55 and 56; Regulation 4; Guidance Note on Information Officers and Deputy Information Officers*	Article 31	
	International data transfer restrictions	Section 57(1),(d) and 72	Articles 14(2), 17(3), 39-12 and 39-13	Chapter 2, Article 9
SCOPE	Exemption for employee data	Section 32(1)(f)		
	Nonprofits covered	Section 3	Article 58	Chapter 1, Article 2
	Sectoral law carveouts		Article 6	Chapter 7, Article 28
	State-level preemption			Chapter 7, Article 28
ENFORCEMENT	Independent enforcement authority	Information Regulator	Personal Information Protection Commission	Personal Data Protection Authority
		Sections 39–54	Article 7	Chapter 6, Articles 19 and 20
	Rulemaking authority	Sections 40(1)(f), 60-68 and 112(2)	Articles 7-8 and 7-9	Chapter 6, Article 22
	Fining authority	Section 109	Articles 70–76	Chapter 5, Article 18; Chapter 6, Article 22
	Criminal penalties	Section 107	Articles 70–73	Chapter 5, Article 17
	Personal liability	Section 93(b)(ii) (Information Officers); Guidance Note on Information Officers and Deputy Information Officers*	Articles 70–76	Chapter 5, Article 18
	Private right of action	Section 99	Articles 51–57	Chapter 3, Article 11(1)(ğ)

***Data breach notification:** *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

***South Africa:** *Access to personal informatiom is further regulated by the Promotion of Access to Information Act No. 2 of 2000. Guidelines, guidance notes and notices from the Information Regulator can be found here.*

iapp

Global Comprehensive Privacy Law Mapping Chart

Last updated: *April 2022*

Note: *This tool is for informational purposes and is not legal advice. Whether a law includes a particular provision should always be verified via official sources.*

		United States				
		California		Colorado	Utah	Virginia
		California Consumer Privacy Act California Consumer Privacy Act Regulations	California Privacy Rights Act (fully operative Jan. 1, 2023)	Colorado Privacy Act* (effective July 1, 2023)	Utah Consumer Privacy Act (effective Dec. 31, 2023)	Virginia's Consumer Data Protection Act (effective Jan. 1, 2023)
INDIVIDUAL RIGHTS	Right to access	Section 1798.100 Section 1798.110 Section 1798.115	Section 1798.100 Section 1798.110 Section 1798.115	Section 6-1-1306(1)(b)	Section 13-61-201(1)	Section 59.1-577(A)(1)
	Right to correct		Section 1798.106	Section 6-1-1306(1)(c)		Section 59.1-577(A)(2)
	Right to delete	Section 1798.105	Section 1798.105	Section 6-1-1306(1)(d)	Section 13-61-201(2)	Section 59.1-577(A)(3)
	Right to portability	Sections 1798.100(d) and 1798.130(a)(2)	Section 1798.130(a)(3)(B)(iii)	Section 6-1-1306(1)(e)	Section 13-61-201(3)	Section 59.1-577(A)(4)
	Right to opt out of all or specific processing	Section 1798.120	Section 1798.120	Section 6-1-1306(1)(a)	Section 13-61-201(4)	Section 59.1-577(A)(5)
	Right to opt in for sensitive data processing		Section 1798.121*	Section 6-1-1308(7)	Section 16-61-302(3)(a) (notice and opportunity to opt-out)	Section 59.1-578(A)(5)
	Age-based opt-in right	Section 1798.120(c)	Section 1798.120(c)	Section 6-1-1308(7)	Section 13-61-302(3)(b) (process in accordance with the Children's Online Privacy Protection Act))	Section 59.1-578(A)(5) (process in accordance with the Children's Online Privacy Protection Act)
	Right not to be subject to fully automated decisions		Section 1798.185(a)(16)*	Section 6-1-1306(1)(a)(I)(C)		Section 59.1-577(A)(5)
BUSINESS OBLIGATIONS	Notice/transparency requirements	Section 1798.100(b) Sections 1798.130(a) and 1798.135	Section 1798.100(a) Section 1798.130	Section 6-1-1308(1)	Section 13-61-302(1)	Section 59.1-578(C)-(E)
	Legal basis for processing					
	Purpose limitation	Section 1798.100(b)	Section 1798.100(c)	Section 6-1-1308(2), (4)		Section 59.1-578(A)(2)
	Data minimization		Sections 1798.100(c) and 1798.100(a)(d)	Section 6-1-1308(3)		Section 59.1-578(A)(1)
	Security requirements	Section 1798.150(a)	Sections 1798.100(e) and 1798.150(a)	Section 6-1-1308(5)	Section 13-61-302(2)	Section 59.1-578(A)(3)
	Privacy by design					
	Processor/service provider requirements	Section 1798.140(v)	Sections 1798.100(d) and 1798.140(ag)(1)	Section 6-1-1305	Section 13-61-301	Section 59.1-579
	Prohibition on discrimination	Section 1798.125	Section 1798.125	Section 6-1-1308(6)	Section 13-61-302(4)	Section 59.1-578(A)(4)
	Record keeping	CCPA Regulations, Section 999.317				
	Risk/impact assessments		Section 1798.185(a)(15)	Section 6-1-1309		Section 59.1-580
	Data breach notification*					
	Registration with authorities					
	Data protection officer					
	International data transfer restrictions					
SCOPE	Exemption for employee data	Section 1798.145(m) from CPRA operative immediately until Jan. 1, 2023		Section 6-1-1304(2)(k) (employment records)*	Section 13-61-102(2)(o)*	Section 59.1-576(C)(14)*
	Nonprofits covered			Section 6-1-1304		
	Sectoral law carveouts	Sections 1798.145 and 1798.146	Sections 1798.145 and 1798.146	Section 6-1-1304(2)	Section 13-61-102(2)	Section 59.1-576
	Preemption	Section 1798.180	Section 1798.180	Section 6-1-1312	Section 13-61-103(1)	
ENFORCEMENT	Independent enforcement authority		California Privacy Protection Agency* Section 1798.199.10 et seq.			
	Rulemaking authority	Section 1798.185	Section 1798.185	Section 6-1-1313		
	Fining authority	Section 1798.155	Sections 1798.155, 1798.199.55 and 1798.199.90	Section 6-1-1311	Section 13-61-402	Section 59.1-584
	Criminal penalties					
	Personal liability					
	Private right of action	Section 1798.150	Section 1798.150			

***Data breach notification:** *Many countries and all 50 U.S. states have separate data breach notification laws. The term in this chart refers to a provision included in a comprehensive data protection law.*

***California:** *The CPRA categorizes sensitive data and allows consumers to limit its use and disclosure but does not require opt-in consent for use of sensitive data. There is no explicit right against automatic decision-making but the use of automatic decision-making is within the scope of the regulations to be promulgated. The CPPA has administrative authority to implement and enforce the CPRA. The California attorney general's office retains civil enforcement authority.*

***Colorado:** *The CPA is now codified in the Colorado Revised Statutes. The definition of "consumer" in Section 6-1-1303(6)(b) "does not include an individual acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context."*

***Utah:** *In addition to the exemption for data processed in the employment context, the definition of "consumer" in Section 13-61-101(10)(b) "does not include an individual acting in an employment or commercial context."*

***Virginia:** *The definition of "consumer" in Section 59.1-575 "does not include a natural person acting in a commercial or employment context."*

IBM **Security**

Cost of a Data Breach Report 2021

IBM

Executive summary

Now in its 17th year, the Cost of a Data Breach Report has become one of the leading benchmark reports in the cybersecurity industry. This report offers IT, risk management and security leaders a lens into dozens of factors that can increase or help mitigate the rising cost of data breaches.

With research conducted independently by the Ponemon Institute, this report – sponsored, analyzed, and published by IBM Security – studied 537 real breaches across 17 countries and regions and 17 different industries.

In the course of nearly 3,500 interviews, we asked dozens of questions to determine what organizations spent on activities for the discovery of and the immediate response to the data breach.

Other issues covered include:

1. Initial attack vectors that were primarily responsible for causing the breaches
2. The length of time it took the organizations to detect and contain their breaches
3. The effects of incident response and security artificial intelligence (AI) and automation on the average total cost

Each year, we aim to renew the report to offer analysis that builds upon past years' research while breaking new ground to keep up with changing technology and events to form a more relevant picture of the risks and strategies for securing data and responding to a breach. The 2021 edition of this report has new analysis related to the advancement of the zero trust approach, risks that continue to make cloud security essential, and the acceleration of remote working as a result of the pandemic.

The report is divided into six major sections, including:

— This executive summary with key findings and comments about how data breach costs were calculated

— A deep dive into the report's complete findings, with dozens of charts

— An exploration of a methodology for risk quantification

— Security recommendations that can help organizations mitigate the financial impacts of a breach

— Notes on the geographic, industry and company size characteristics of the organizations studied

— And a more detailed explanation of the study's methodology and limitations

IBM Security and the Ponemon Institute are pleased to present the results of the 2021 Cost of a Data Breach Report.

Years in this report refer to the year the report was published, not necessarily the year the breach occurred. Breaches in the 2021 report took place between May 2020 and March 2021.

Key findings

The key findings described here are based on IBM Security analysis of the research data compiled by the Ponemon Institute.

10%

Increase in average total cost of a breach, 2020-2021

The average total cost of a data breach increased by nearly 10% year over year, the largest single year cost increase in the last seven years.

Data breach costs rose from $3.86 million to $4.24 million, the highest average total cost in the history of this report. Costs were significantly lower for some of organizations with a more mature security posture, and higher for organizations that lagged in areas such as security AI and automation, zero trust and cloud security.

Note: Cost amounts in this report are measured in U.S. dollars.

$1.07m

Cost difference where remote work was a factor in causing the breach

Remote working and digital transformation due to the COVID-19 pandemic increased the average total cost of a data breach.

The average cost was $1.07 million higher in breaches where remote work was a factor in causing the breach, compared to those where remote work was not a factor. The percentage of companies where remote work was a factor in the breach was 17.5%. Additionally, organizations that had more than 50% of their workforce working remotely took 58 days longer to identify and contain breaches than those with 50% or less working remotely. IT changes such as cloud migration and remote work increased costs, yet organizations that did not implement any digital transformation changes as a result of COVID-19 experienced $750,000 higher costs compared to the global average, a difference of 16.6%.

11

Consecutive years healthcare had the highest industry cost of a breach

Healthcare organizations experienced the highest average cost of a data breach, for the eleventh year in a row.

Healthcare data breach costs increased from an average total cost of $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase. Costs varied widely across industries, and year over year. Costs in the energy sector decreased from $6.39 million in 2020 to an average $4.65 million in 2021. Costs surged in the public sector, which saw a 78.7% increase in average total cost from $1.08 million to $1.93 million.

38%

Lost business share of total breach costs

Lost business represented the largest share of breach costs, at an average total cost of $1.59M.

Lost business represented 38% of the overall average and increased slightly from $1.52 million in the 2020 study. Lost business costs included increased customer turnover, lost revenue due to system downtime and the increasing cost of acquiring new business due to diminished reputation.

$180

Per record cost of personally identifiable information

Customer personally identifiable information (PII) was the most common type of record lost, included in 44% of breaches.

Customer PII was also the costliest record type, at $180 per lost or stolen record. The overall average cost per record in the 2021 study was $161, an increase from $146 per lost or stolen record in the 2020 report year.

20%

Share of breaches initially caused by compromised credentials

Compromised credentials was the most common initial attack vector, responsible for 20% of breaches.

Business email compromise (BEC) was responsible for only 4% of breaches, but had the highest average total cost of the 10 initial attack vectors in the study, at $5.01 million. The second costliest was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million).

287

Average number of days to identify and contain a data breach

The longer it took to identify and contain, the more costly the breach.

Data breaches that took longer than 200 days to identify and contain cost on average $4.87 million, compared to $3.61 million for breaches that took less than 200 days. Overall, it took an average of 287 days to identify and contain a data breach, seven days longer than in the previous report. To put this in perspective, if a breach occurring on January 1 took 287 days to identify and contain, the breach wouldn't be contained until October 14th. The average time to identify and contain varied widely depending on the type of data breach, attack vector, factors such as the use of security AI and automation, and cloud modernization stage.

100x

Cost multiplier of > 50 million records vs. average breach

Average cost of a mega breach was $401 million for breaches between 50 million and 65 million records, an increase from $392 million in 2020.

In a small sample of mega breaches of 1 million to 65 million records, breaches were many times more expensive than the average cost of smaller breaches. Breaches of 50 million to 65 million records were nearly 100x more expensive than breaches of 1,000-100,000 records.

$1.76m

Cost difference in breaches where mature zero trust was deployed vs. no zero trust

A zero trust approach helped reduce the average cost of a data breach.

The average cost of a breach was $5.04 million for those without zero trust deployed. Yet in the mature stage of zero trust deployment, the average cost of a breach was $3.28 million, $1.76 million less than organizations without zero trust, representing a 2.3% difference.

80%

Cost difference where security AI and automation was fully deployed vs. not deployed

Security AI and automation had the biggest positive cost impact.

Organizations with fully deployed security AI and automation experienced breach costs of $2.90 million, compared to $6.71 million at organizations without security AI and automation. The difference of $3.81 million, or nearly 80%, represents the largest gap in the study when comparing breaches with vs. without a particular cost factor. The share of organizations with fully or partially deployed security AI and automation was 65% in 2021 vs. 59% in 2020, a 6 percentage point increase and continuing an upward trend. Security AI/automation was associated with a faster time to identify and contain the breach.

$3.61m

Average cost of a breach in hybrid cloud environments

Hybrid cloud had the lowest average total cost of a data breach, compared to public, private and on premise cloud models.

Data breaches in hybrid cloud environments cost an average of $3.61 million, $1.19 million less than public cloud breaches, or a difference of 28.3%. While companies that were in the midst of a large cloud migration experienced higher breach costs, those that were further along in their cloud modernization maturity were able to identify and contain breaches 77 days faster than those in the early stages of modernization.

$2.30m

Cost difference for breaches with high vs. low level of compliance failures

System complexity and compliance failures were top factors amplifying data breach costs.

Organizations with a high level of system complexity had an average cost of a breach $2.15 million higher than those who had low levels of complexity. The presence of a high level of compliance failures was associated with breach costs that were $2.30 million higher than breach costs at organizations without this factor present.

$4.62m

Average total cost of a ransomware breach

Ransomware and destructive attacks were costlier than other types of breaches.

Ransomware attacks cost an average of $4.62 million, more expensive than the average data breach ($4.24 million). These costs included escalation, notification, lost business and response costs, but did not include the cost of the ransom. Malicious attacks that destroyed data in destructive wiper-style attacks cost an average of $4.69 million. The percentage of companies where ransomware was a factor in the breach was 7.8%.

How we calculate the cost of a data breach

To calculate the average cost of a data breach, this research excludes very small and very large breaches. Data breaches examined in the 2021 study ranged in size between 2,000 and 101,000 compromised records. We use a separate analysis to examine the costs of very large "mega breaches," which we explore in further detail in the complete findings section of the report.

This research uses an accounting method called activity-based costing, which identifies activities and assigns a cost according to actual use. Four process-related activities drive a range of expenditures associated with an organization's data breach: detection and escalation, notification, post breach response and lost business.

For a more in-depth explanation of the methods used for this report, see the section on research methodology.

The four cost centers

Detection and escalation

Activities that enable a company to reasonably detect the breach.

- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards

Notification

Activities that enable the company to notify datasubjects, data protection regulators and other third parties.

- Emails, letters, outbound calls or general notice to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement of outside experts

Lost business

Activities that attempt to minimize the loss of customers, business disruption and revenue losses.

- Business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers
- Reputation losses and diminished goodwill

Post breach response

Activities to help victims of a breach communicate with the company and redress activities to victims and regulators.

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fine

Complete findings

In this section, we provide the detailed findings of this research. Topics are presented in the following order:

1. Global findings and highlights
2. Initial attack vectors
3. Lifecycle of a breach
4. Regulatory compliance failures
5. Impact of zero trust
6. Security AI and automation
7. Cloud breaches and migration
8. COVID-19 and remote work
9. Cost of a mega breach

Global findings and highlights

The Cost of a Data Breach Report is a global report, combining results from 537 organizations across 17 countries and regions, and 17 industries to provide global averages. However, in some cases, the report breaks out the results by country/region or industry for comparative purposes. Although sample sizes in some countries/regions and industries are quite small, the organizations in the study have been selected in an attempt to be representative.

Key finding

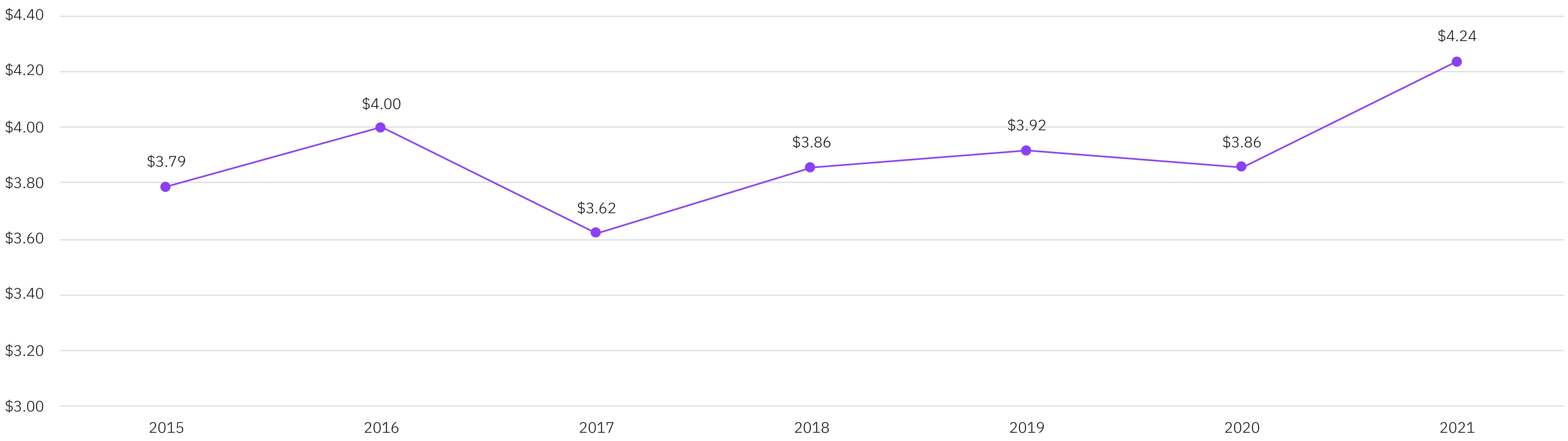
$4.24m

Global average total cost of a data breach

Figure 1

Average total cost of a data breach

Measured in US$ millions



The average total cost of a data breach increased by the largest margin in seven years.

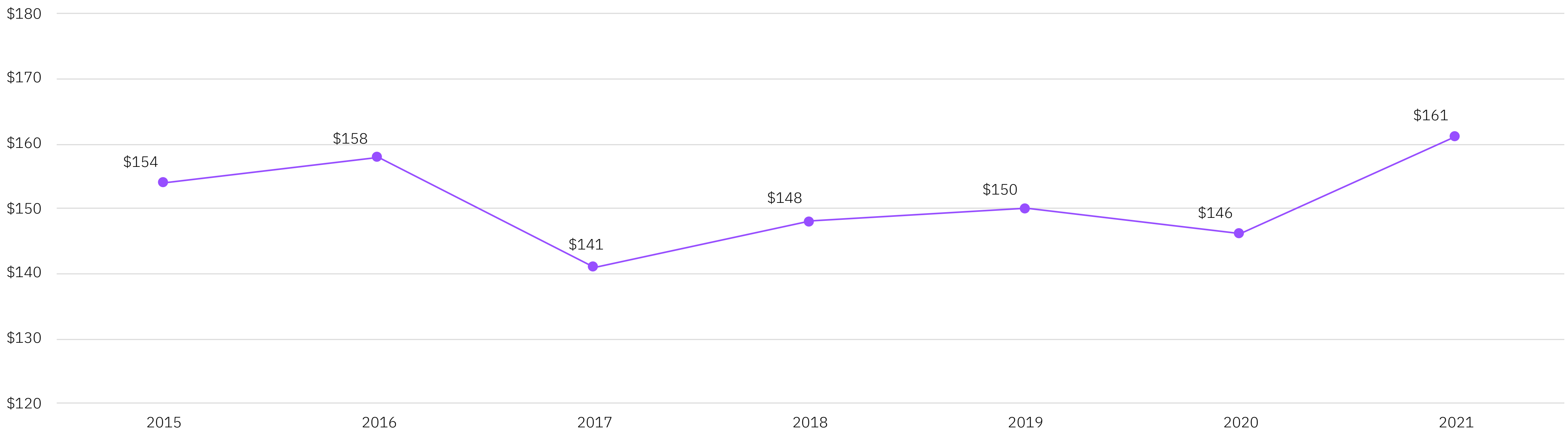
Data breach costs increased significantly year-over year from the 2020 report to the 2021 report, increasing from $3.86 million in 2020 to $4.24 million in 2021.

The increase of $0.38 million ($380,000) represents a 9.8% increase. This compares to a decrease of 1.5% from the 2019 to 2020 report year. The cost of a data breach has increase by 11.9% since 2015.

Figure 2

Average per record cost of a data breach

Measured in US$



The average per record (per capita) cost of a data breach increased 10.3% from 2020 to 2021.

In 2021 the per record cost of a breach was $161, compared to an average cost of $146 in 2020. This represents an increase of 14.2% since the 2017 report, when the average per record cost was $141.

*It is not consistent with this research to use the per record cost to calculate the cost of single or multiple breaches above 100,000 records. For more information, see the research methodology section.

Figure 3

Average total cost of a data breach by country or region

Measured in US$ millions

The United States was the top country for average total cost of a data breach for the eleventh year in a row.

The top five countries and regions for average total cost of a data breach were:

1. U.S.
2. Middle East
3. Canada
4. Germany
5. Japan

These same five countries comprised the top five countries in the 2020 report, in the same order. The average total cost in the U.S. increased from $8.64 million in 2020 to $9.05 million in 2021. The Middle East increased from $6.52 million to $6.93M and Canada increased from $4.50M in 2020 to $5.40 million in 2021. Countries with the largest average total cost increase from 2020 to 2021 include Latin America (52.4% increase), South Africa (50% increase), Australia (30.2% increase), Canada (20% increase), the UK (19.7% increase), and France (14% increase). Only one country in the study saw a cost decrease, Brazil (3.6% decrease). One region, ASEAN, saw no change in average total cost ($2.71 million, no change in 2021).

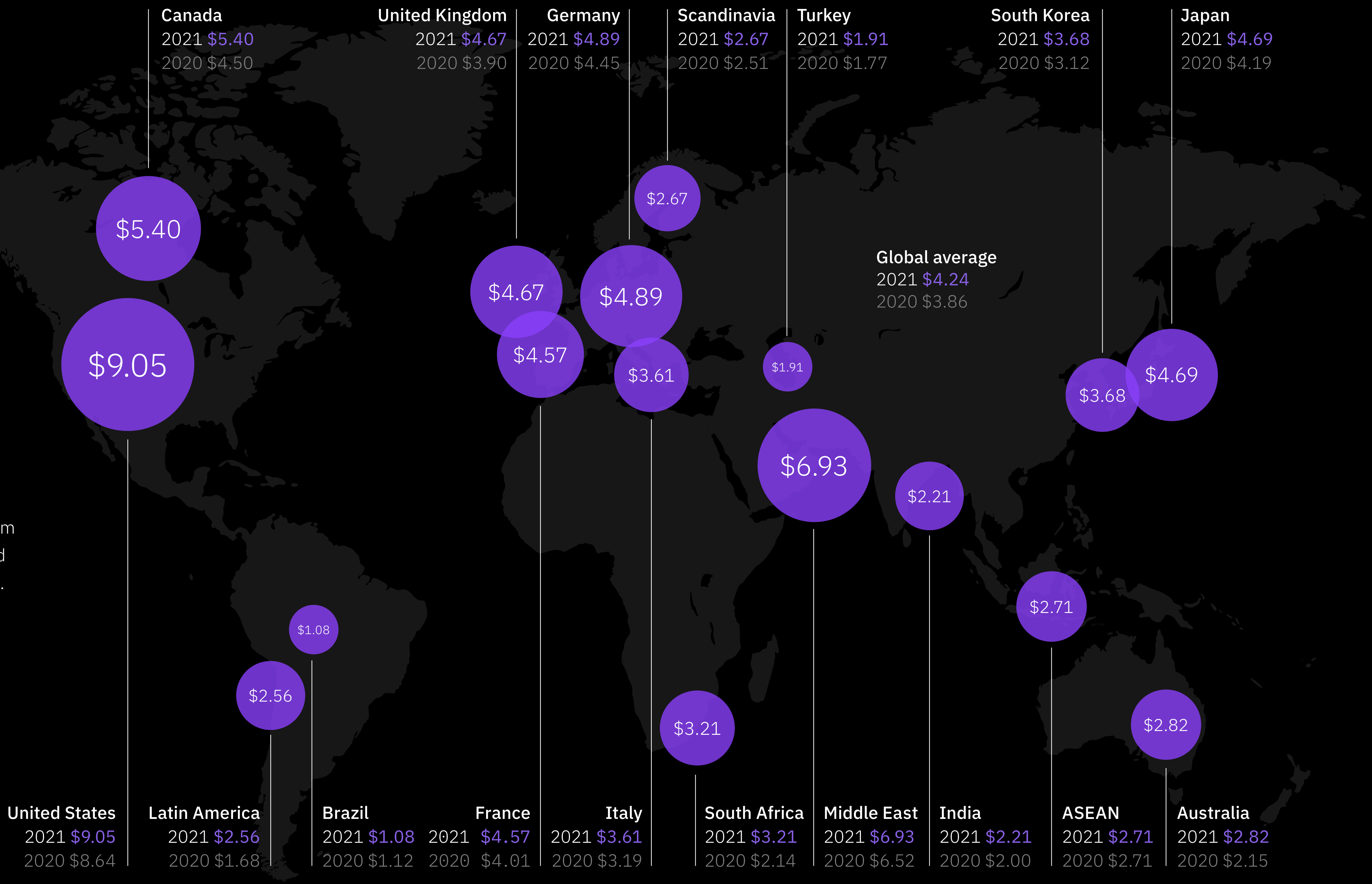
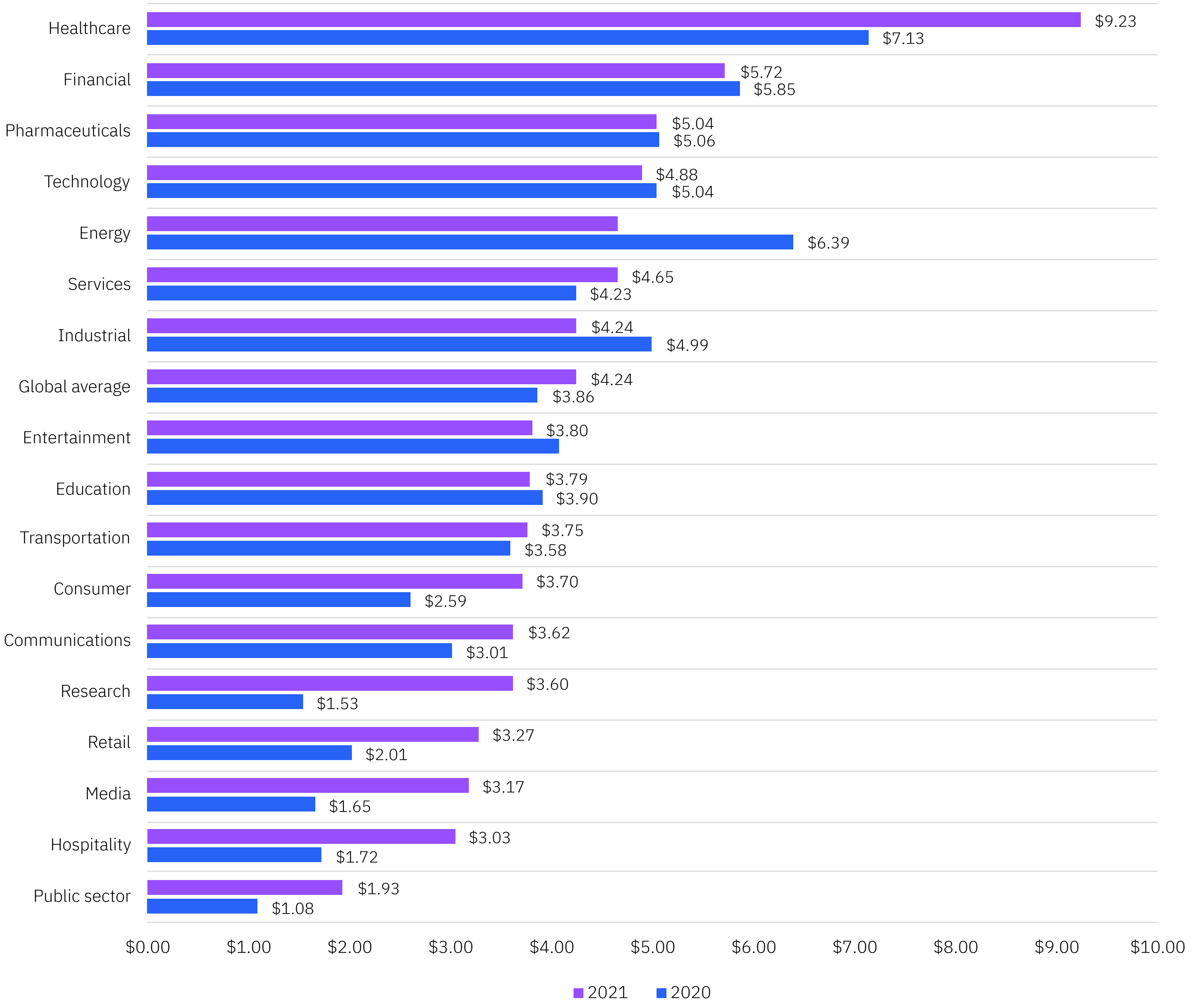


Figure 4

Average total cost of a data breach by industry

Measured in US$ millions



Healthcare was the top industry in average total cost for the eleventh year in a row.

The top five industries for average total cost were:

1. Healthcare
2. Financial
3. Pharmaceuticals
4. Technology
5. Energy

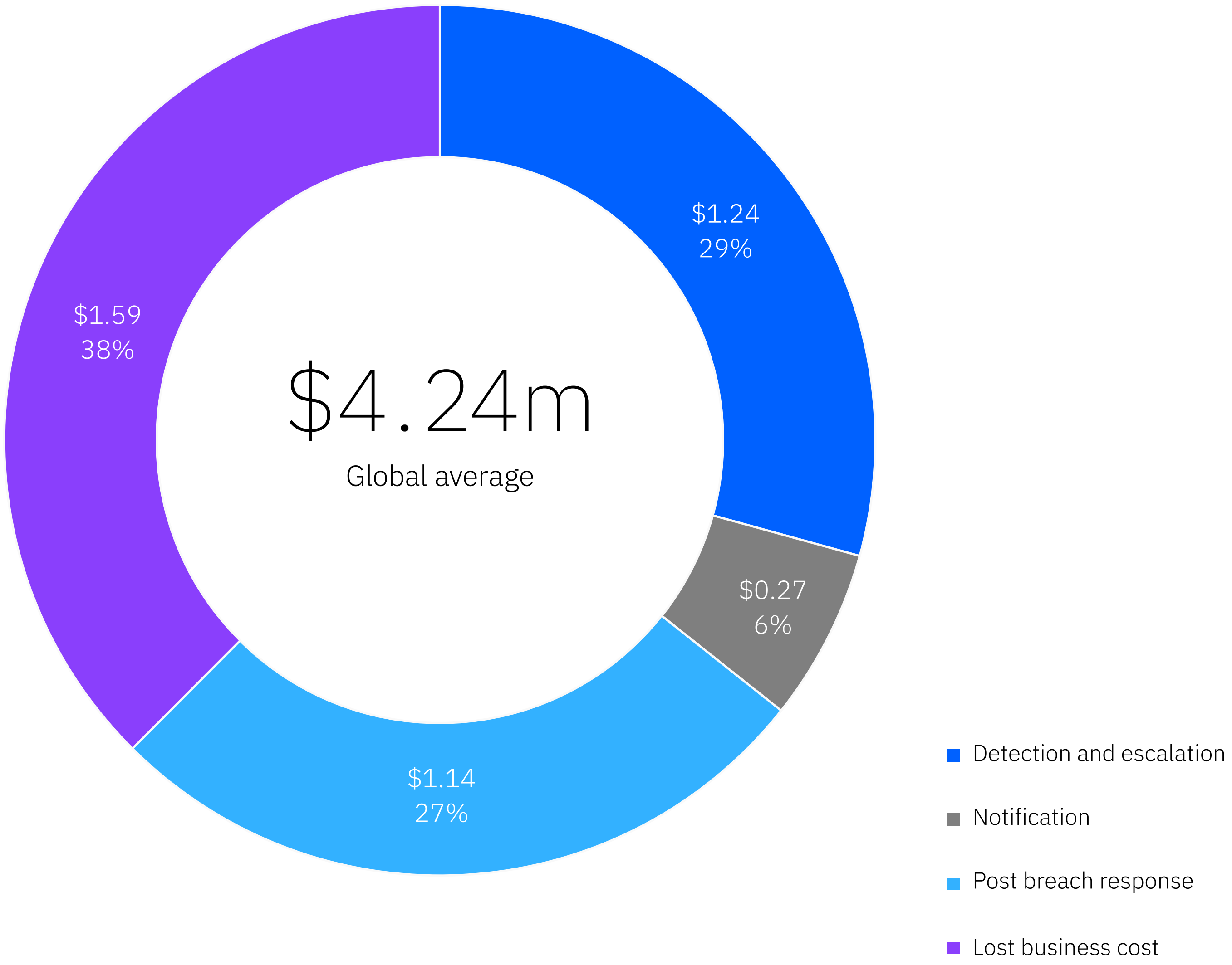
The average total cost for healthcare increased from $7.13 million in 2020 to $9.23 million in 2021, a 29.5% increase. Energy dropped from the second most costly industry to fifth place, decreasing in cost from $6.39 million in 2020 to $4.65 million in 2021 (27.2% decrease).

Other industries that saw large cost increases included services (7.8% increase), communications (20.3% increase), consumer (42.9% increase), retail (62.7% increase), media (92.1% increase), hospitality (76.2% increase), and public sector (78.7% increase).

Figure 5

Average total cost of a data breach divided into four categories

Measured in US$ millions



Lost business continued to represent the largest share of data breach costs for the seventh year in a row.

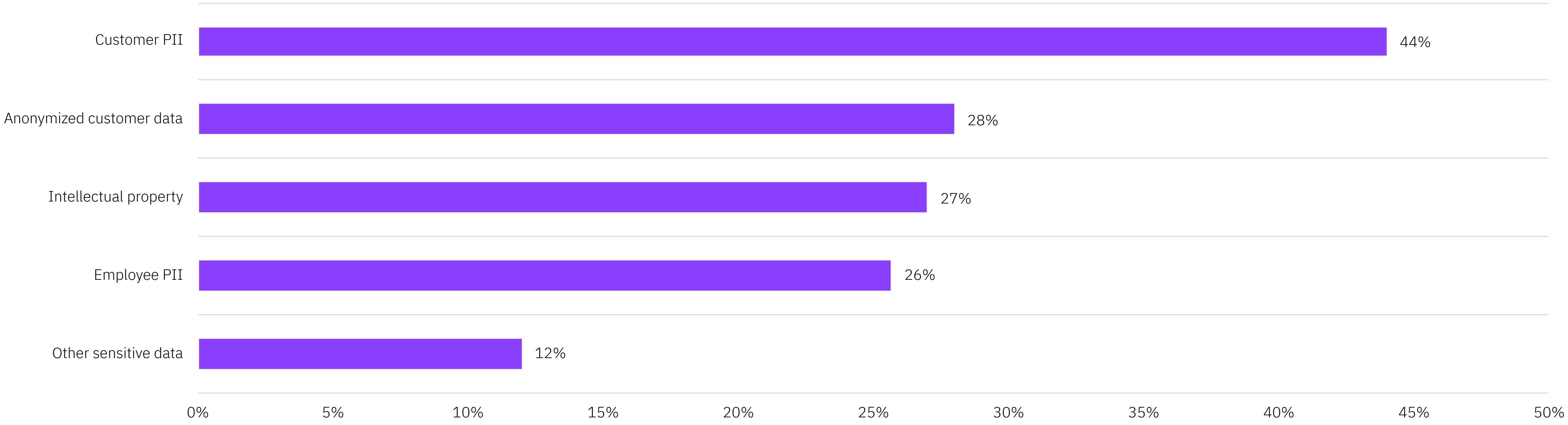
Of the four cost categories, at an average total cost of $1.59 million, lost business accounted for 38% of the average total cost of a data breach. Lost business costs include: business disruption and revenue losses from system downtime, cost of lost customers and acquiring new customers, reputation losses and diminished goodwill.

The second most costly was detection and escalation costs, which had an average total cost of $1.24 million, or 29% of the total cost. The other cost categories are notification and post data breach response.

Figure 6

Types of records compromised

Percentage of breaches involving data in each category



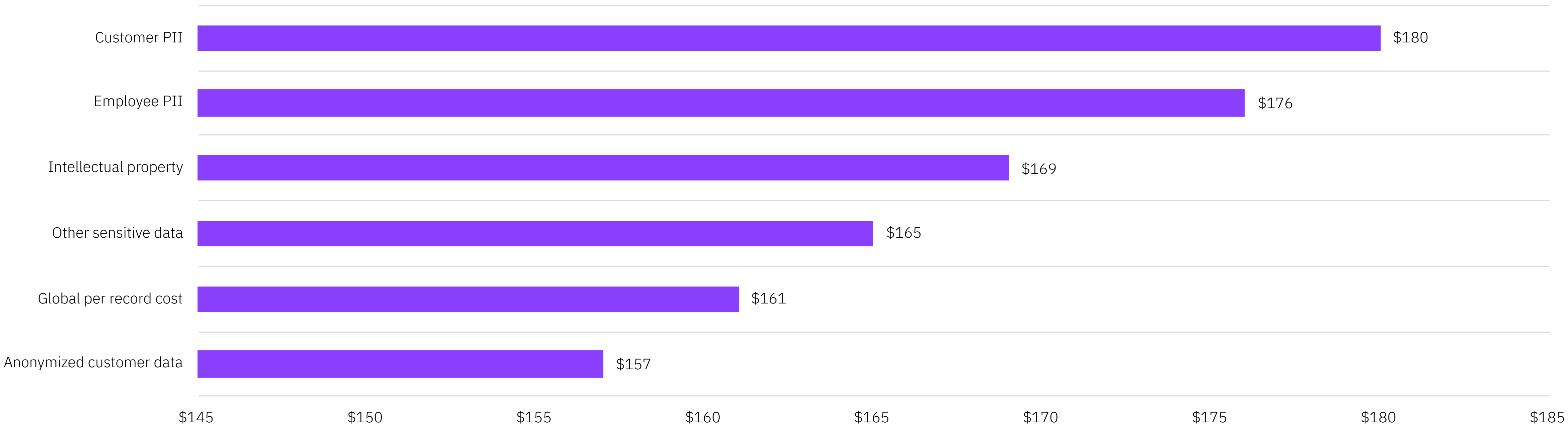
Customer personally identifiable information (PII) was the most common type of record lost or stolen.

Customer PII was included in 44% of all breaches in the study. Anonymized customer data (i.e., data that is modified to remove PII) was compromised in 28% of the breaches studied, the second most common type of record compromised in breaches.

Figure 7

Average cost per record by type of data compromised

Measured in US$



Customer PII was the costliest type of record lost or stolen in breaches.

Customer PII cost an average of $180 per lost or stolen record in 2021. In 2020, customer PII cost $150 per lost or stolen record, representing an increase of 20%.

Initial attack vectors

This section looks at the prevalence and cost of initial attack vectors of data breaches. The breaches in the study are divided into 10 initial attack vectors, ranging from accidental data loss and cloud misconfiguration to phishing, insider threats, and lost or stolen (i.e., compromised) credentials.

Key finding

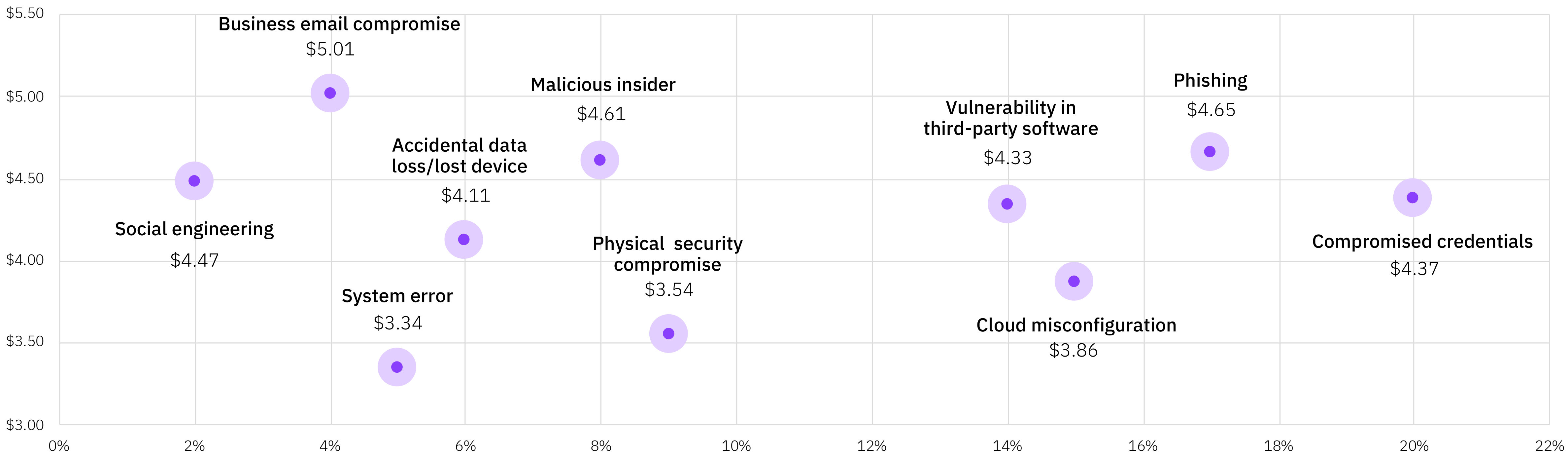
$5.01m

Average total cost of a breach caused by business email compromise

Figure 8

Average total cost and frequency of data breaches by initial attack vector

Measured in US$ millions



The most common initial attack vector in 2021 was compromised credentials, responsible for 20% of breaches.

In 2021, the most frequent initial attack vectors were (1) compromised credentials, 20% of breaches (2) phishing, 17% (3) cloud misconfiguration, 15%. Business email compromise was responsible for only 4% of breaches but had the highest average total cost at $5.01 million. The second costliest initial attack vector was phishing ($4.65 million), followed by malicious insiders ($4.61 million), social engineering ($4.47 million), and compromised credentials ($4.37 million). The top four initial attack vectors were the same in 2021 as compared to the 2020 study, but slightly re-ordered. Phishing moved up from fourth to second most common, and cloud misconfiguration fell from second to third-most common. Vulnerabilities in third-party software (average cost of $4.33 million) fell from third to fourth in frequency, a category that was the initial attack vector in 14% of breaches in 2021, compared to about 16% of breaches in 2020.

Lifecycle of a breach

The time elapsed between the first detection of the breach and its containment is referred to as the data breach lifecycle. The average time to identify describes the time it takes to detect that an incident has occurred. The time to contain refers to the time it takes for an organization to resolve a situation once it has been detected and ultimately restore service. These metrics can be used to determine the effectiveness of an organization's incident response and containment processes.

Key finding

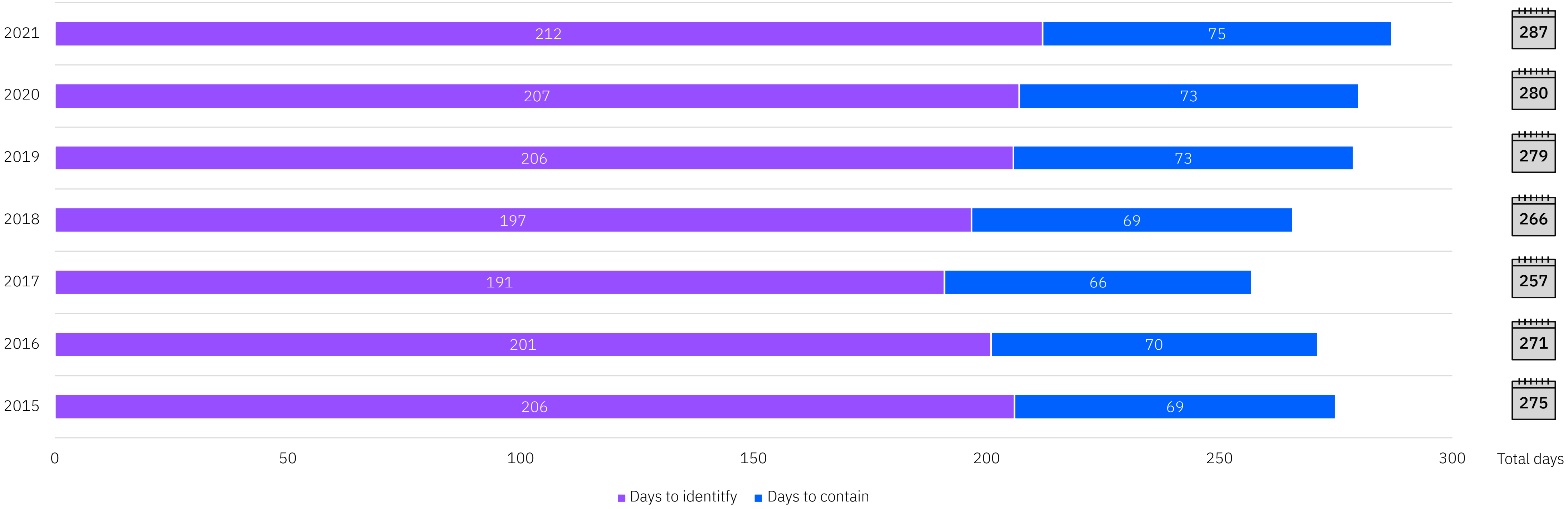
$4.87m

Average cost of a breach with a lifecycle over 200 days

Figure 9

Average time to identify and contain a data breach

Measured in days



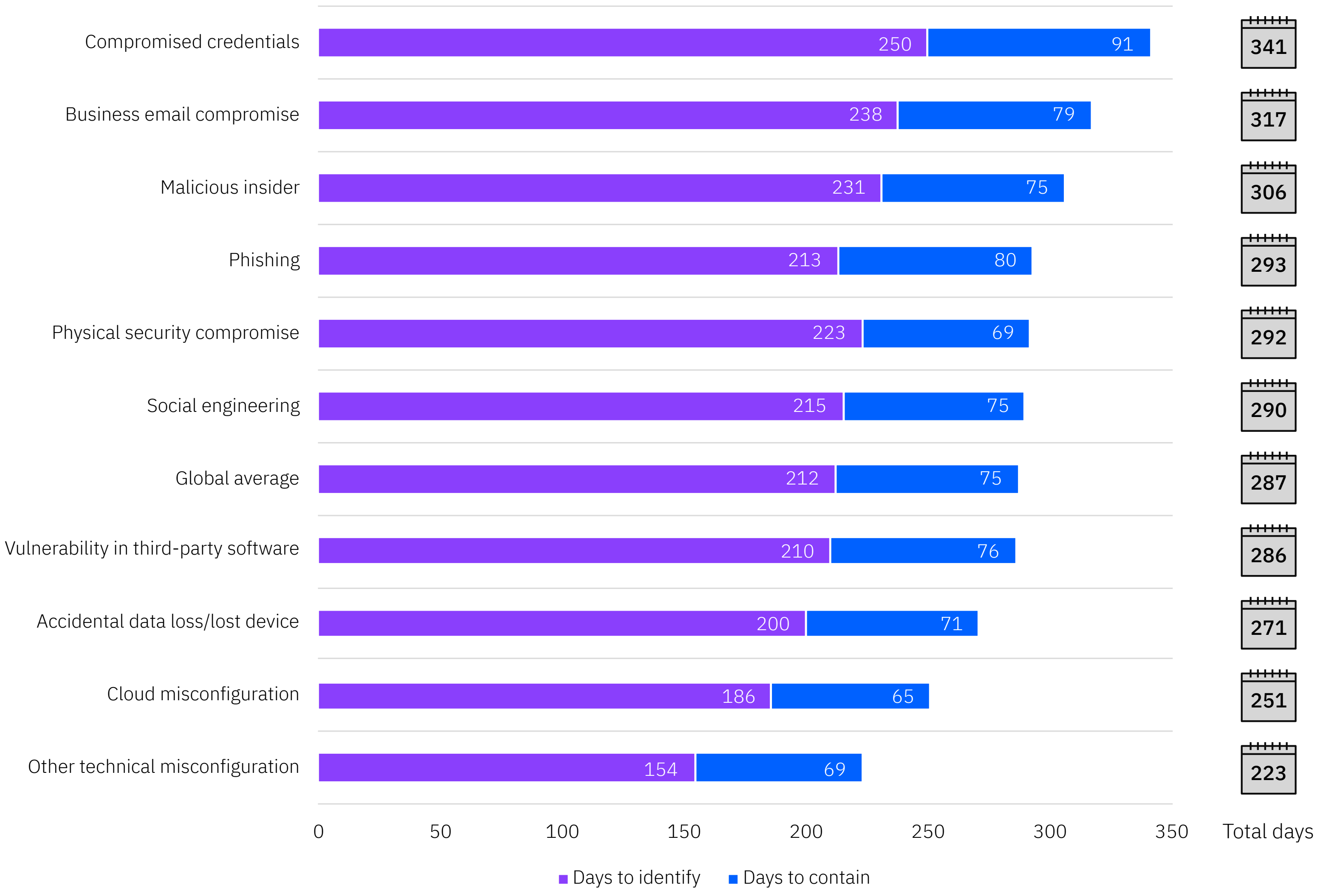
The data breach lifecycle took a week longer in 2021 than in 2020.

In 2021 it took an average of 212 days to identify a breach and an average 75 days to contain a breach, for a total lifecycle of 287 days. If a breach occurred on January 1st and it took 287 days to identify and contain, the breach would not be contained until October 14th.

Figure 10

Average time to identify and contain a breach by initial attack vector

Measured in days



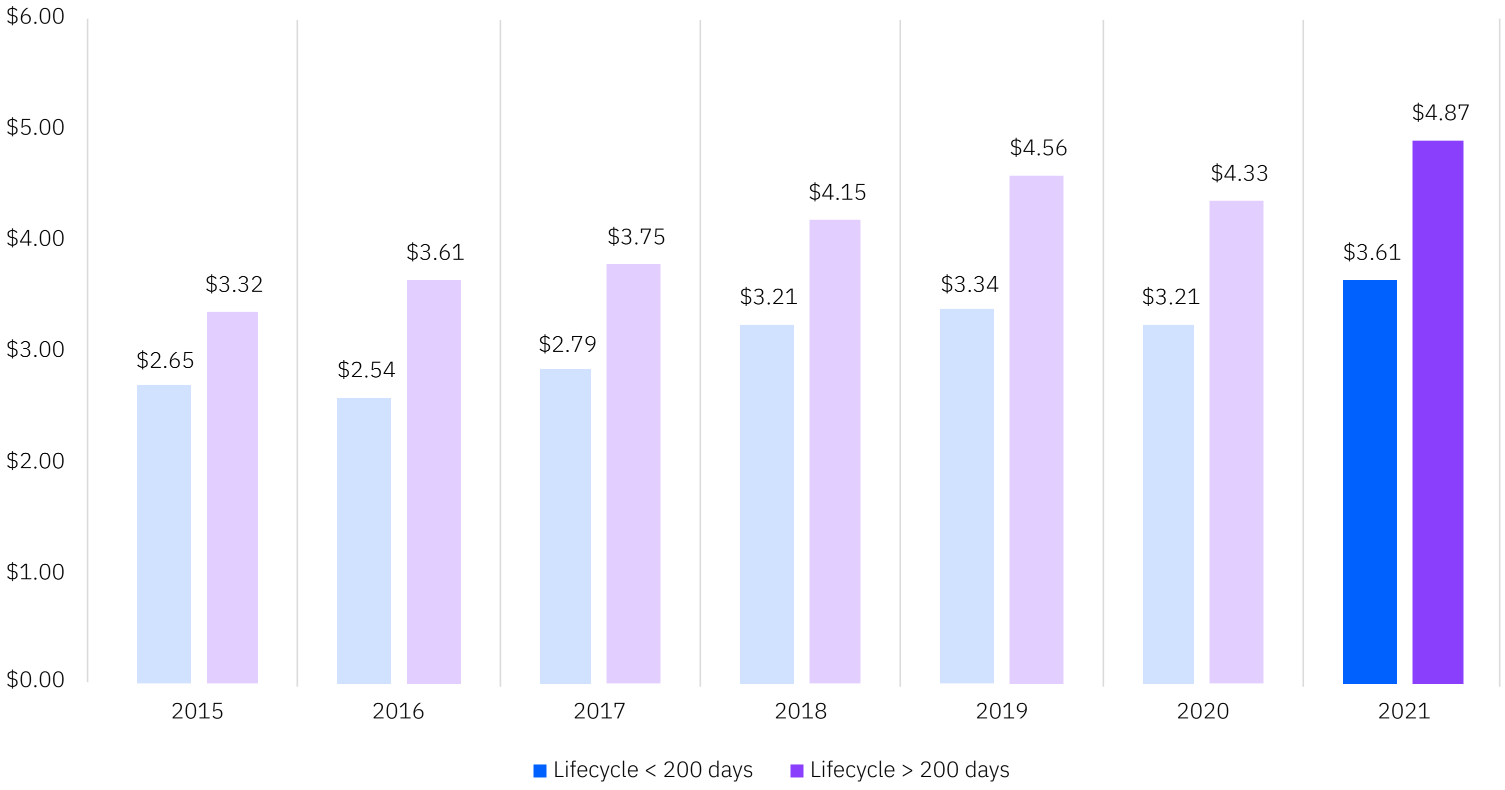
On average, a breach caused by stolen credentials that occurred on January 1st would take until December 7 to be contained.

Breaches caused by stolen/compromised credentials took the longest number of days to identify (250) and contain (91) on average, for an average total of 341 days. Business email compromise had the second longest breach lifecycle at 317 days and malicious insider breaches took the third longest number of days to identify and contain at 306 days.

Figure 11

Average total cost of a data breach based on average data breach lifecycle

Measured in US$ millions



A data breach lifecycle of less than 200 days produced a cost savings of nearly a third over a breach lifecycle longer than 200 days.

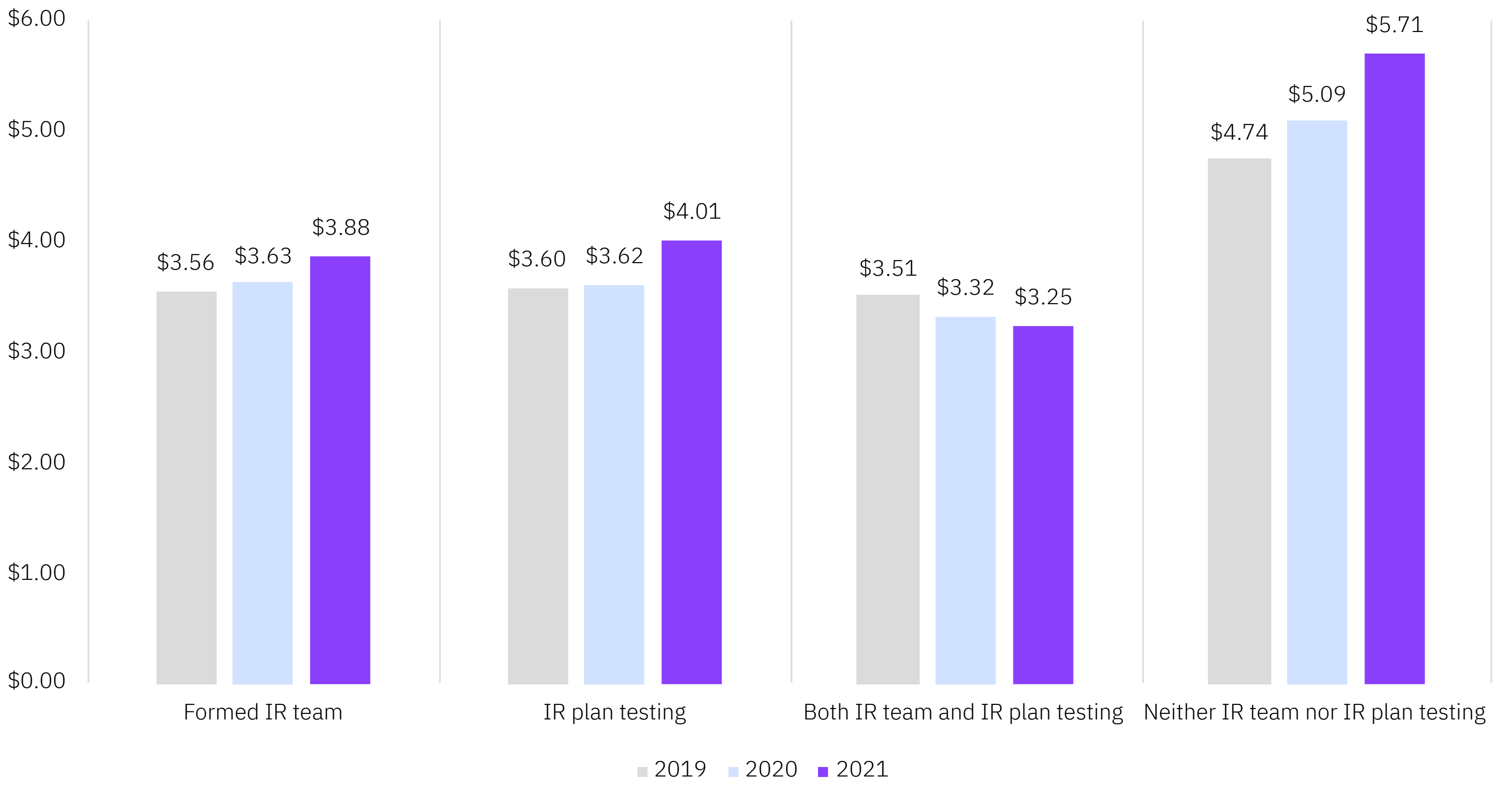
A breach with a lifecycle over 200 days cost an average of $4.87 million in 2021, vs. $3.61 million for a breach with a lifecycle of less than 200 days. The gap of $1.26 million represents a difference of 29.7%. This gap between breaches with a lifecycle shorter/longer than 200 days was $1.12 million in 2020. That means the beneficial cost impact of containment in less than 200 days grew from 2020 to 2021.

Tweet →

Figure 12

Average total cost of a data breach with incident response (IR) team and IR plan testing

Measured in US$ millions



Incident response teams and incident response plan testing continued to mitigate costs in 2021.

The gap in average total cost between breaches at organizations with both IR teams and IR plan testing (IR capabilities), and organization with no IR team and no IR plan testing continued to grow. Breaches at organizations with IR capabilities cost an average of $3.25 million in 2021, compared to $3.32 million in 2020. The average total cost of a breach at organizations with no IR capabilities was $5.71 million in 2021, an increase from $5.09 million in 2020. The average total cost gap between IR capabilities vs. no IR capabilities was $2.46 million in 2021, representing a 54.9% difference.

The average cost difference between breaches at organizations with IR capabilities and organizations without IR capabilities was 42.1% in 2020. This indicates a growing cost difference effectiveness of IR capabilities from 2020 to 2021 (difference of $2.46 million in 2021 vs. $1.77 million in 2020). The average total cost of a breach at organizations with IR capabilities had a difference of 26.4% compared to the overall average total cost of $4.24 million in 2021.

Regulatory compliance failures

This year’s research study looked closely at the impacts of regulatory compliance failures. In this section, we first looked at the impact of compliance failures on the average total cost of a data breach. Out of a selection of 25 cost factors that either amplify or mitigate data breach costs, compliance failures was the top cost amplifying factor.

We then looked at the difference in “longtail costs” in breaches at organizations in highly regulated industries versus those in industries with less stringent data protection regulations. We defined highly regulated industries to include energy, healthcare, consumer goods, financial, technology, pharmaceuticals, communication, public sector and education. Organizations in retail, industrial, entertainment, media, research services, and hospitality were considered to be in a low regulatory environment. In the analysis of industries in the high versus low regulation categories, we concluded that regulatory and legal costs may have contributed to higher costs in the years following a breach.

Key finding

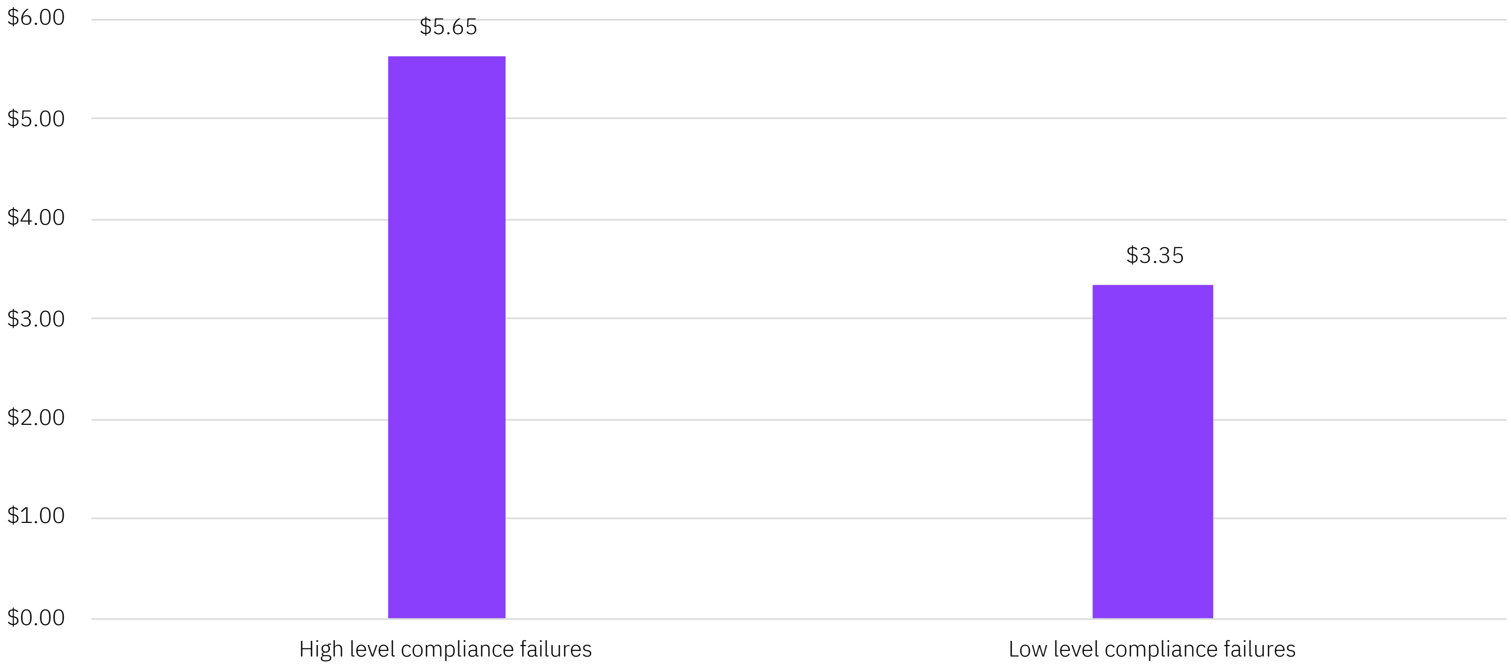
$5.65m

Average cost of a breach at organizations with high level compliance failures

Figure 13

Impact of compliance failures on the average cost of a data breach

Measured in US$ millions



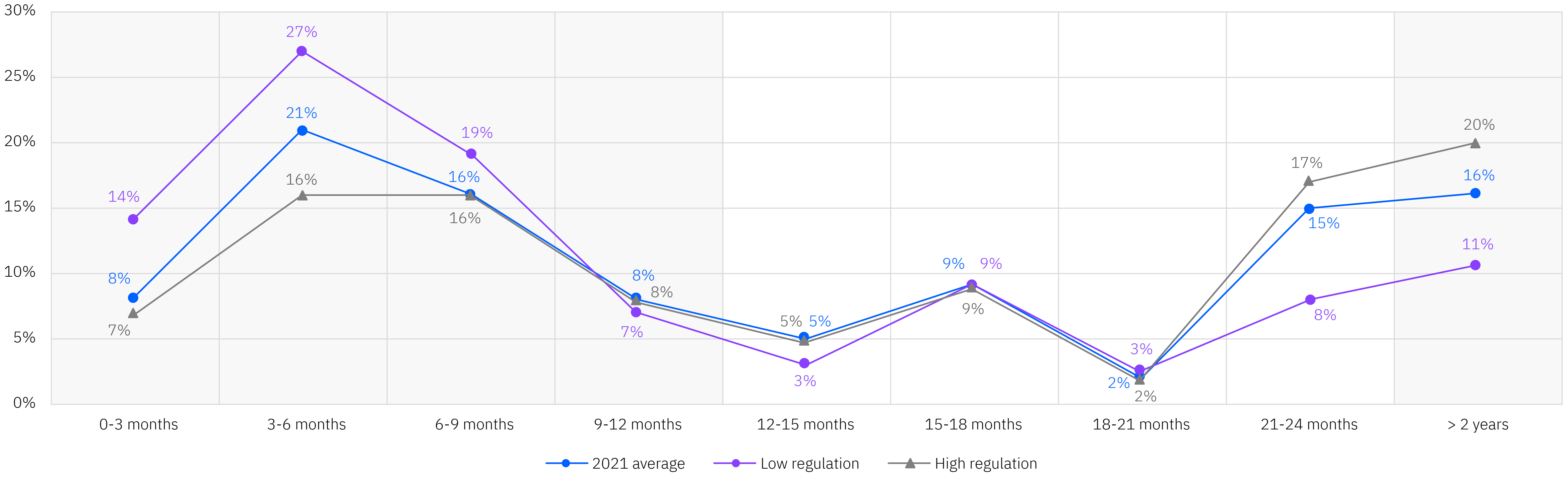
Compliance failures was the top factor found to amplify data breach costs.

Organizations with a high level of compliance failures (resulting in fines, penalties and lawsuits) experienced an average cost of a data breach of $5.65 million, compared to $3.35 million at organizations with low levels of compliance failures, a difference of $2.3 million or 51.1%.

Figure 14

Average distribution of data breach costs over time in low vs. high regulatory environments

Percentage of total costs accrued in three month intervals



Breaches in stricter regulatory environments tended to see more costs accrue in later years following the breach.

The difference between high regulatory environments and low regulatory environments was most pronounced in breach costs incurred more than two years after the breach. In highly regulated industries, 20% of costs were incurred after two years, vs. 11% of costs in less regulated industries. Overall averages found that 16% of breach costs were incurred after two years. In less regulated industries, 68% of costs were incurred in the first 12 months, vs. 46% of costs in highly regulated industries. Note: This research examined a sample of breaches over two-plus years – 83 breaches in a high regulatory environment and 101 in a low regulatory environment.

	2021 avg.	Low	High
Time elapsed	Percentage of total cost		
1st year	53%	67%	47%
2nd year	31%	22%	33%
2+ years	16%	11%	20%

Impact of zero trust

For the first year, this study examined the prevalence and impact of a zero trust security architecture. This approach operates on the assumption that user identities or the network itself may already be compromised, and instead relies on AI and analytics to continuously validate connections between users, data and resources.

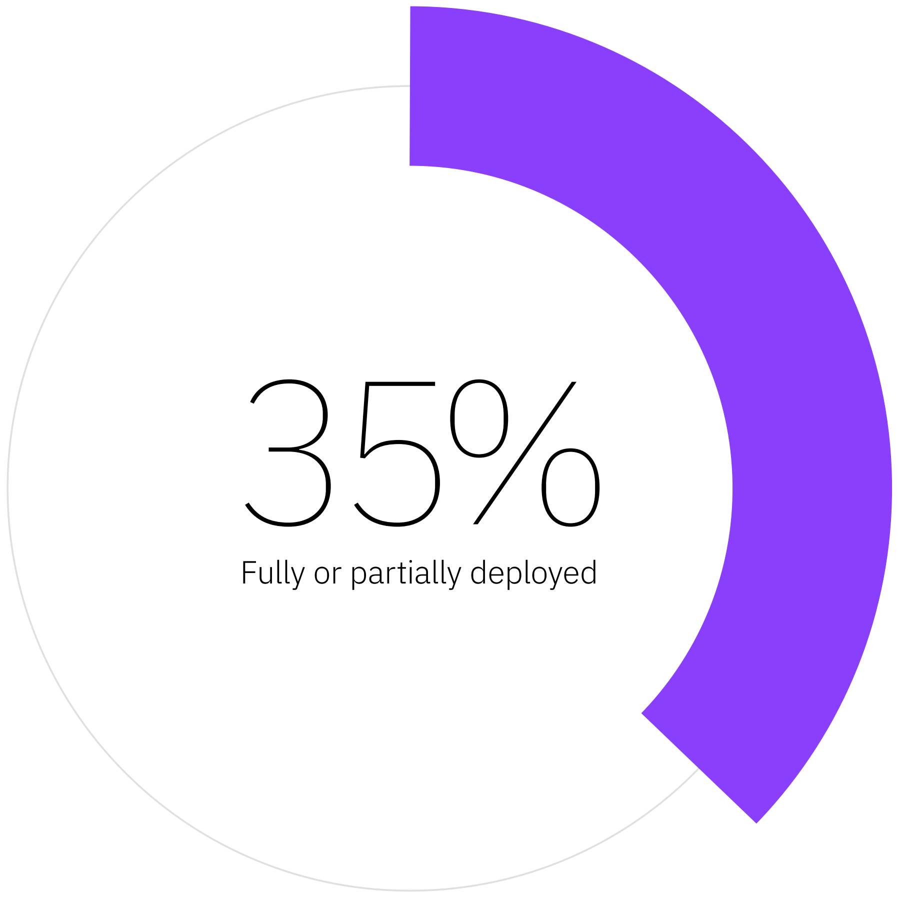
Key finding

$5.04m

Average cost of a breach at organizations without zero trust deployed

Figure 15

Has your organization deployed zero trust?



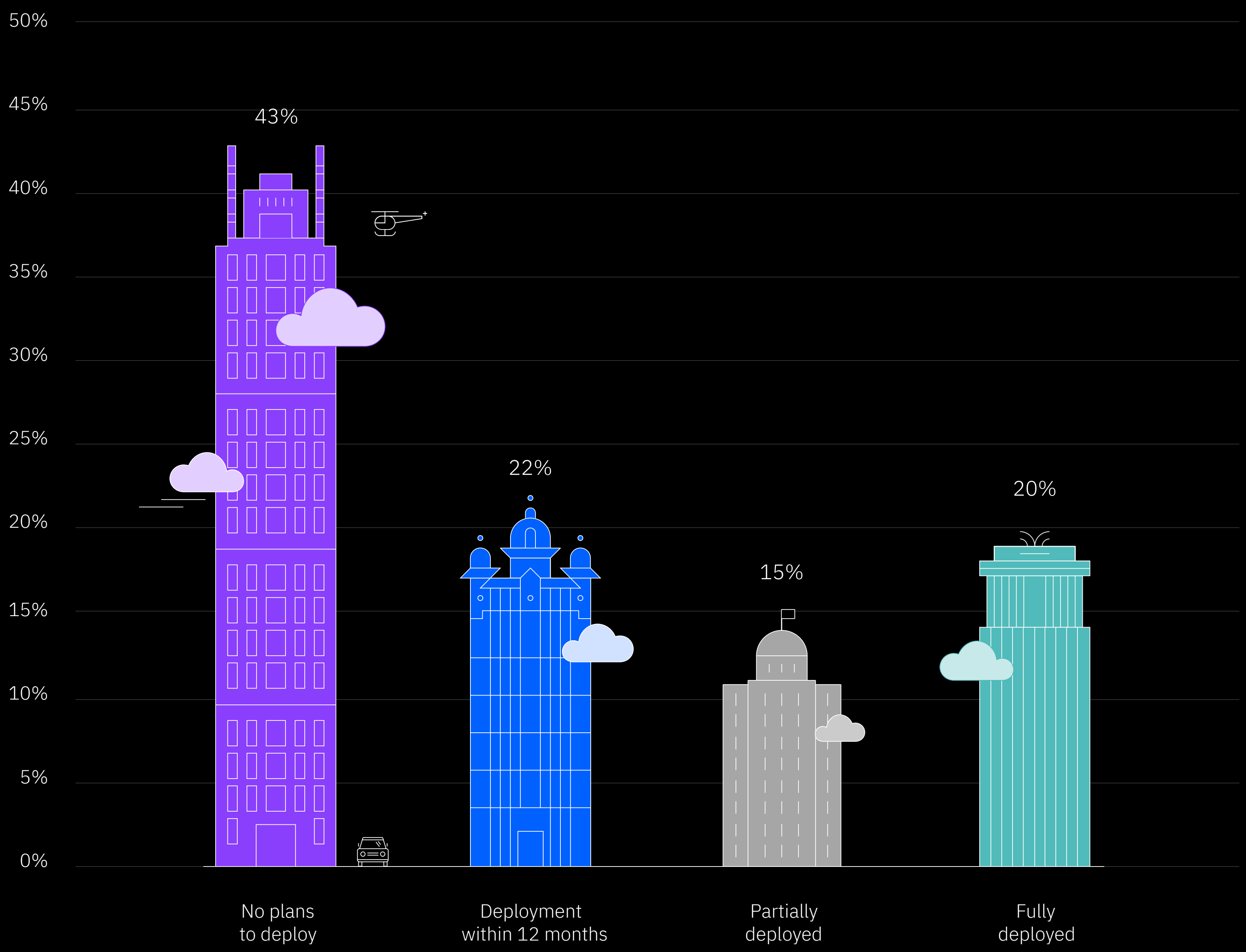
Only about a third of organizations have a zero trust approach.

While 65% of respondents do not have zero trust deployed, 35% have a partially or fully deployed zero trust approach.

Figure 16

State of zero trust deployment

Percentage of organizations per deployment category



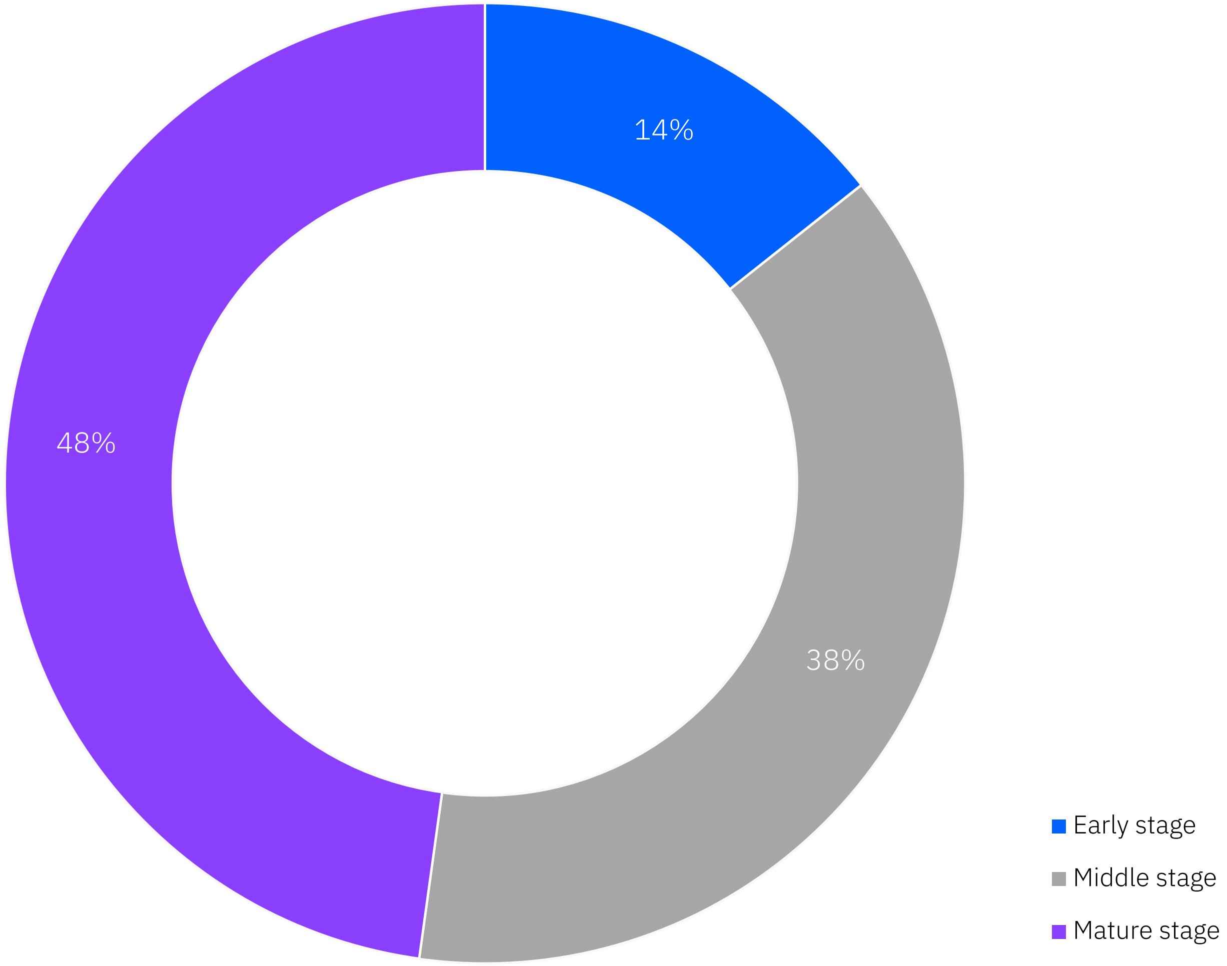
Close to half of organizations have no plans in place to deploy zero trust.

Just 20% are fully deployed and 15% are partially deployed. While 22% say they plan to deploy zero trust in the next 12 months, 43% say they have no current plans to deploy zero trust.

Figure 17

Zero trust maturity level

Percentage of organizations per maturity stage



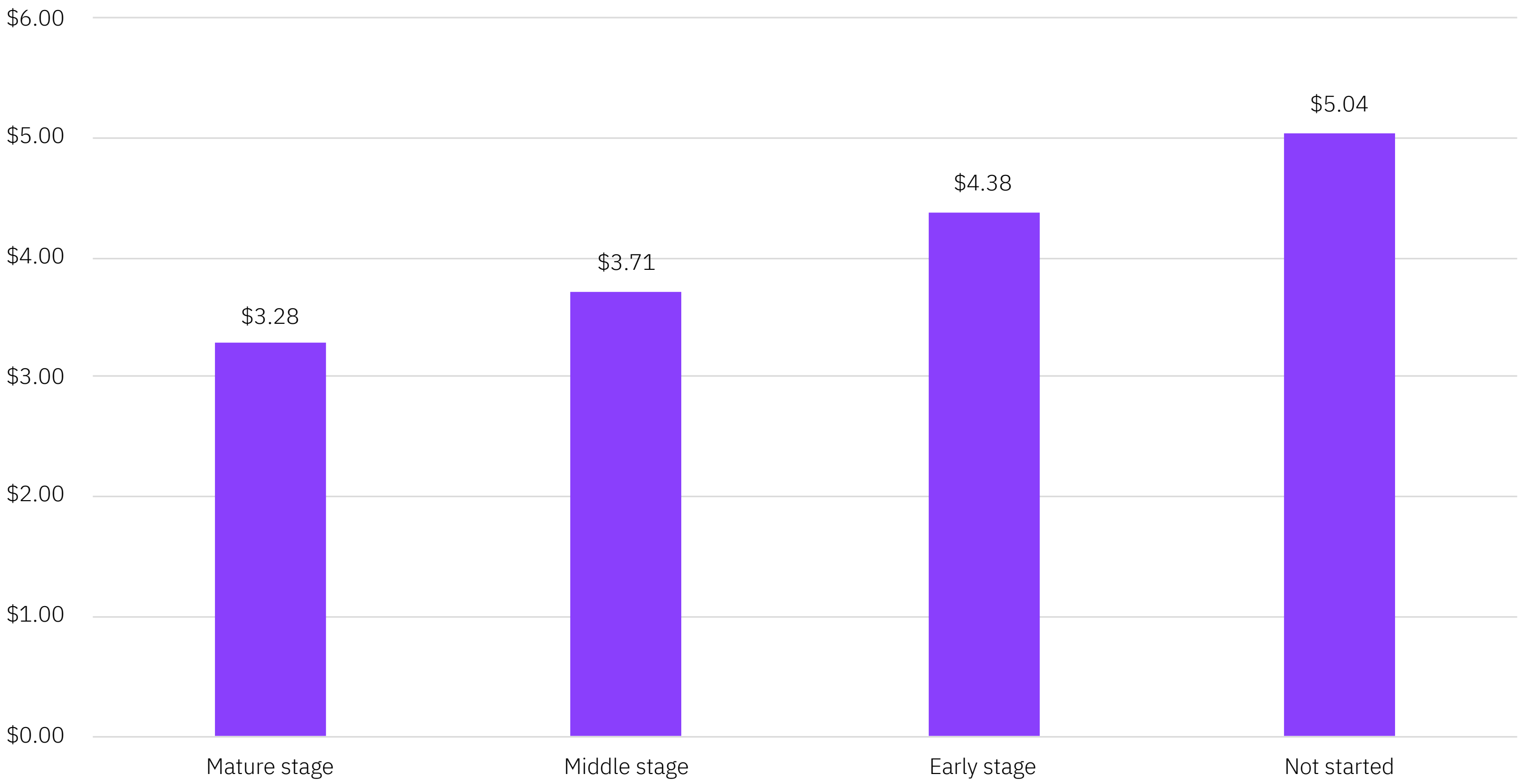
Those who have deployed zero trust tend to be in the middle or mature stages of deployment.

Of respondents that have fully or partially or fully deployed zero trust, 14% are in early stage deployment, 38% middle stage and 48% mature stage. This means just 16.8% of organizations in the study have a mature stage zero trust approach (i.e., 48% of the 35% of respondents that have deployed zero trust).

Figure 18

Average total cost of a breach by the state of zero trust deployment

Measured in US$ millions



Costs stayed lower for organizations in the mature stage of zero trust.

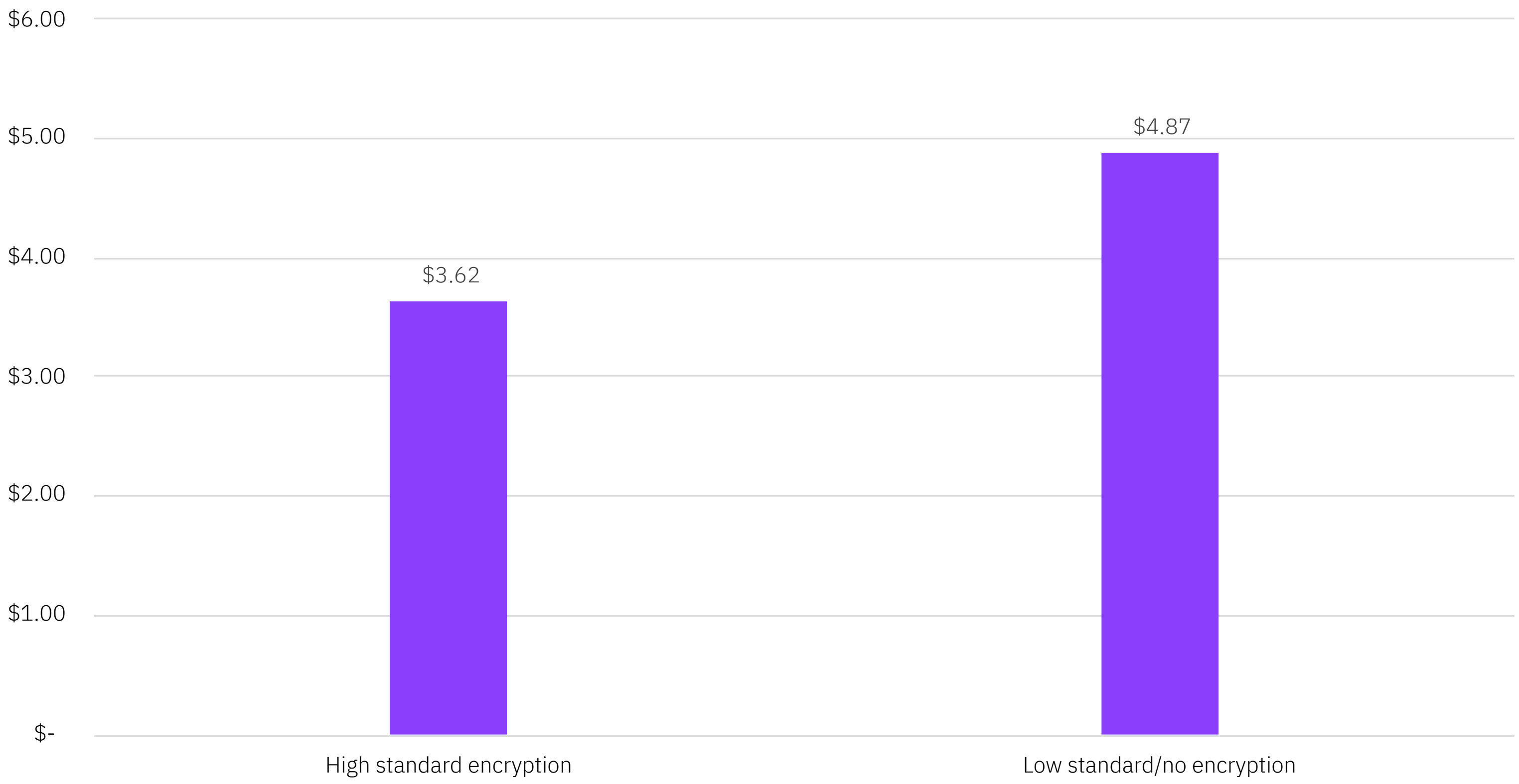
The average cost of a data breach was higher for organizations that had not deployed/not started to deploy zero trust. Costs for those that had zero trust depend on level of maturity. The average cost of a breach was $5.04 million in 2021 for those with no zero trust approach.

In mature stage of deployment, the average cost of a breach was $3.28 million. This difference of $1.76 million between mature zero trust organizations and organizations without zero trust is a cost difference of 42.3%. The difference between early stage zero trust (average cost of a breach $4.38 million) and mature stage ($3.28 million) was $1.10 million, for a cost difference of 28.7%.

Figure 19

Impact of encryption on average cost of a data breach

Measured in US$ millions



Use of strong encryption, a key component of zero trust, was a top mitigating cost factor.

In an analysis of 25 cost factors that either amplified or mitigated the average total cost of a data breach, use of high standard encryption was third among cost mitigating factors, after mature use of AI platforms and mature use of analytics.

Organizations using high standard encryption (using at least 256 AES encryption, at rest and in motion), had an average total cost of a breach of $3.62 million, compared to $4.87 million at organizations using low standard or no encryption, a difference of $1.25M or 29.4%.

Security AI and automation

This was the fourth year we examined the relationship between data breach cost and security automation. In this context, security automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of incidents and intrusion attempts. Such technologies depend upon artificial intelligence, machine learning, analytics and automated security orchestration.

On the opposite end of the spectrum are processes driven by manual inputs, often across dozens of tools and complex, non-integrated systems, without data shared between them. On average, organizations in the study had 34 security tools.

Key finding

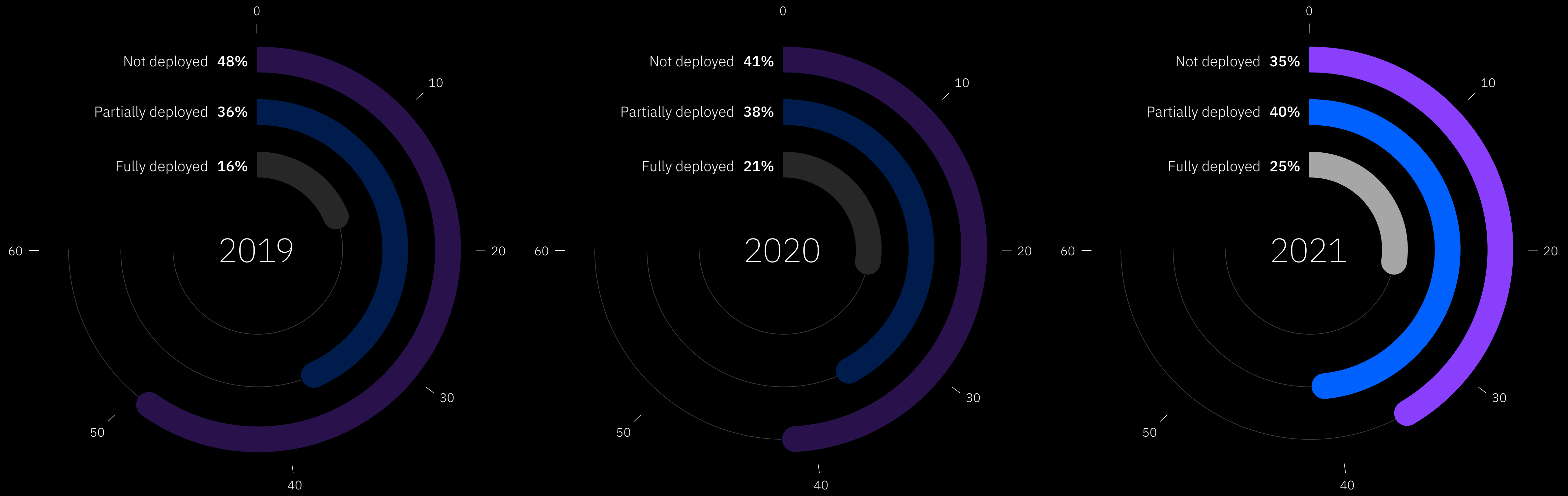
$2.90m

Average cost of a data breach at organizations with security AI and automation fully deployed

Figure 20

State of security AI and automation comparing three levels of deployment

Percentage of organizations per deployment level



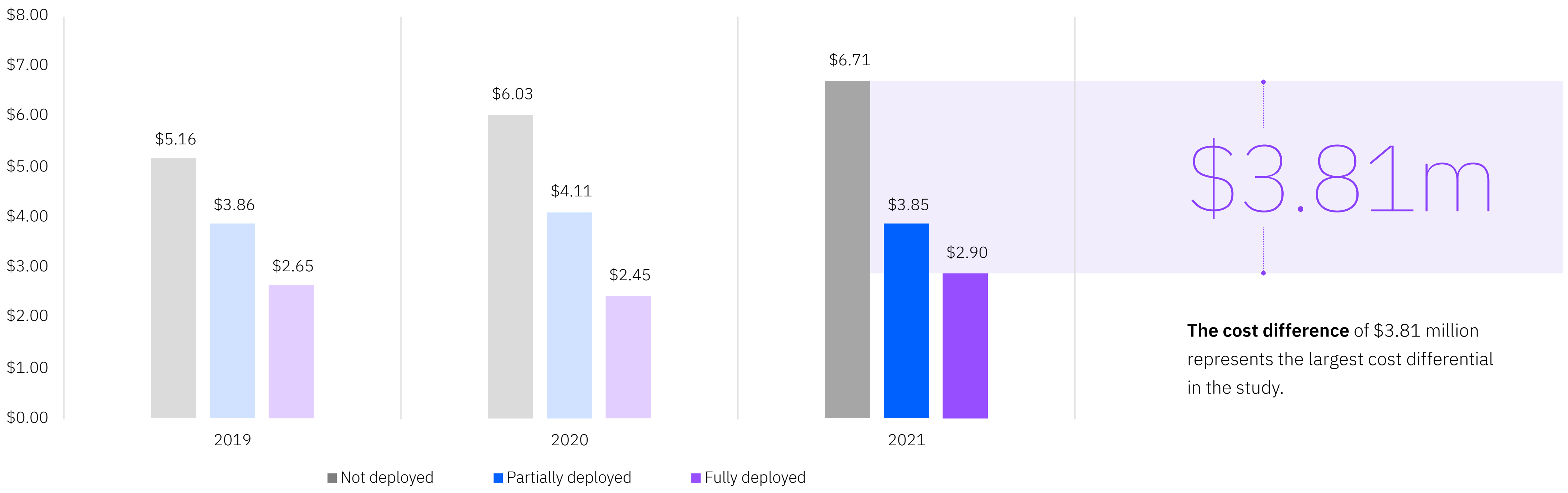
The share of organizations with fully or partially deployed security automation increased by six percentage points.

In 2021, 25% of respondents had fully deployed security automation, vs. 40% partially deployed and 35% not deployed. In 2020, 21% of respondents had fully deployed security automation, vs. 38% partially deployed and 41% not deployed. The share of organizations with fully or partially deployed security automation was 65% in 2021 vs. 59% in 2020. This represents a six percentage point increase in organizations with either fully or partially deployed automation from 2020 to 2021, and a decrease of 6 percentage points in the share of organizations with no security automation deployed.

Figure 21

Average cost of a data breach by security automation deployment level

Measured in US$ millions



The cost difference of $3.81 million represents the largest cost differential in the study.

The biggest cost savings in the study was to organizations with high levels of security AI and automation.

Organizations with no security automation experienced breach costs of $6.71 million on average in 2021, vs. $2.90 million on average at organizations with fully deployed security automation.

In 2020, organizations without security AI/automation saw breach costs of $6.03M, vs. $2.45M with fully deployed security automation, a difference of $3.58 million, or 84.4%. Between 2019 and 2021, the cost of a breach at organizations with fully deployed security automation increased.

Organizations with fully deployed security AI and automation were able to detect and contain a breach must more quickly than organizations with no security AI/automation deployed.

For organizations with fully deployed security AI/automation, it took an average of 184 days to identify the breach and 63 days to contain the breach, for a total lifecycle of 247 days.

For organizations with no security AI/automation deployed, it took an average of 239 days to identify the breach and 85 days to contain, for a total lifecycle of 324 days. The difference in breach lifecycle of 77 days represents a difference of 27%. For fully deployed organizations, a breach occurring on January 1 would on average take until September 4 to identify and contain.

For organizations with no automation deployed, a breach on January 1 would take on average until November 20 to identify and contain.

See figure 22 on page 39 →

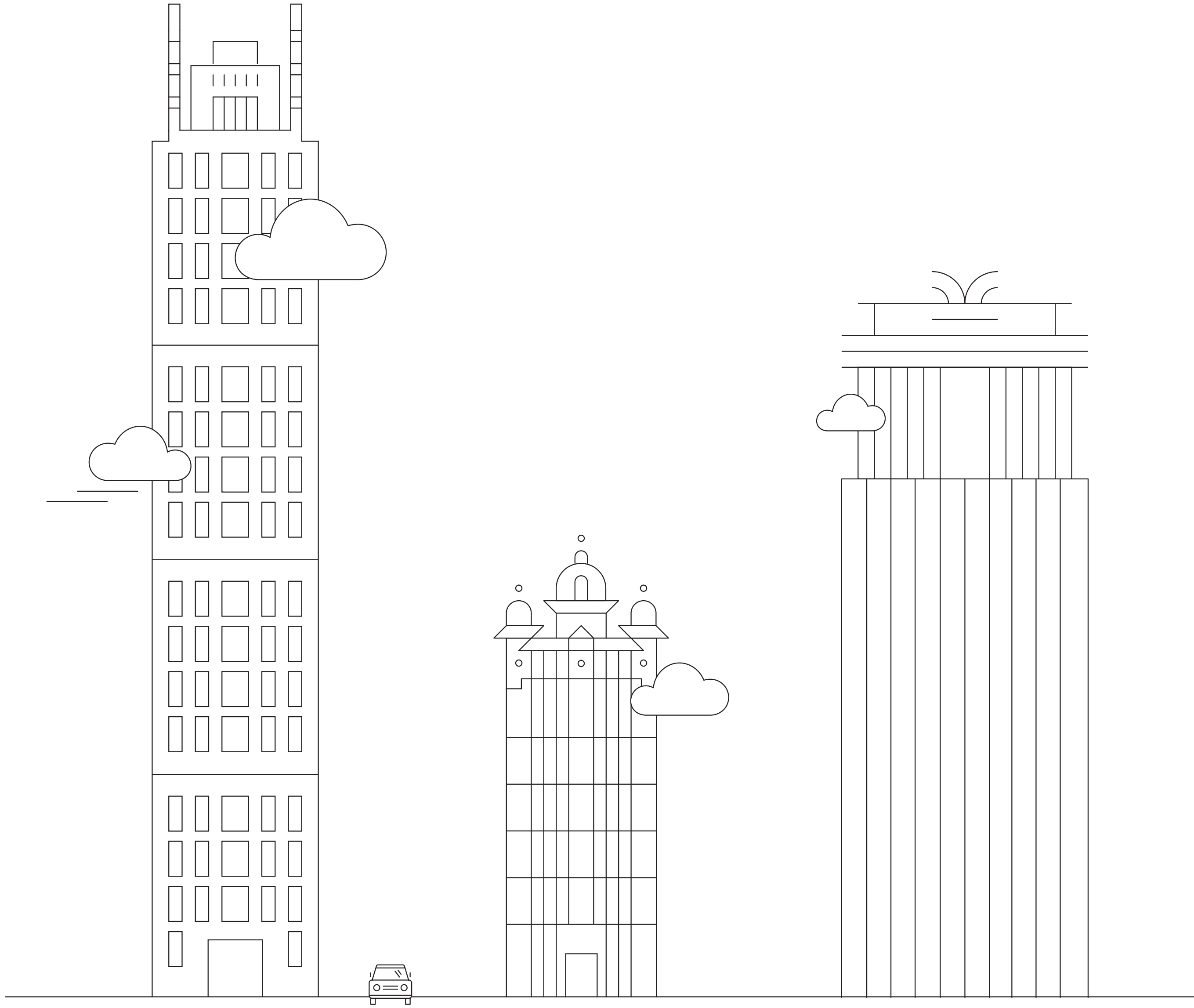


Figure 22

Average time to identify and contain a data breach by level of security automation

Measured in days

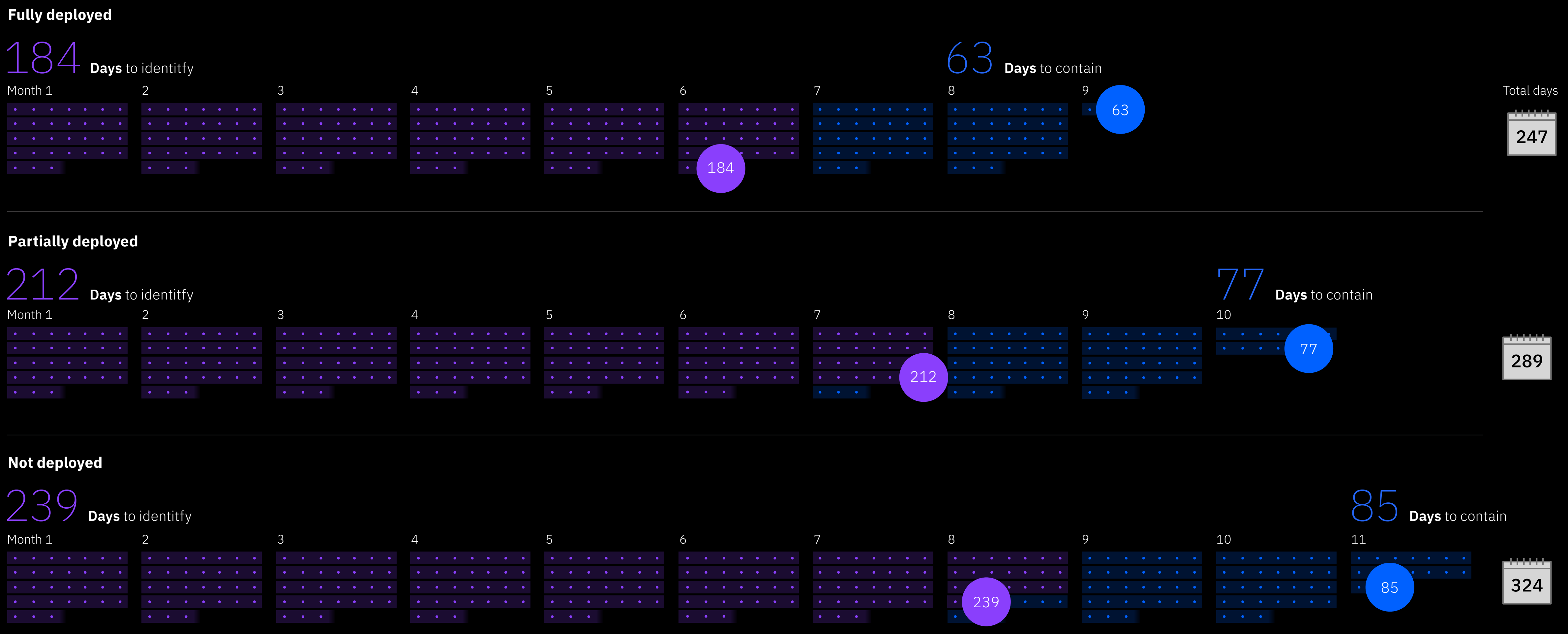
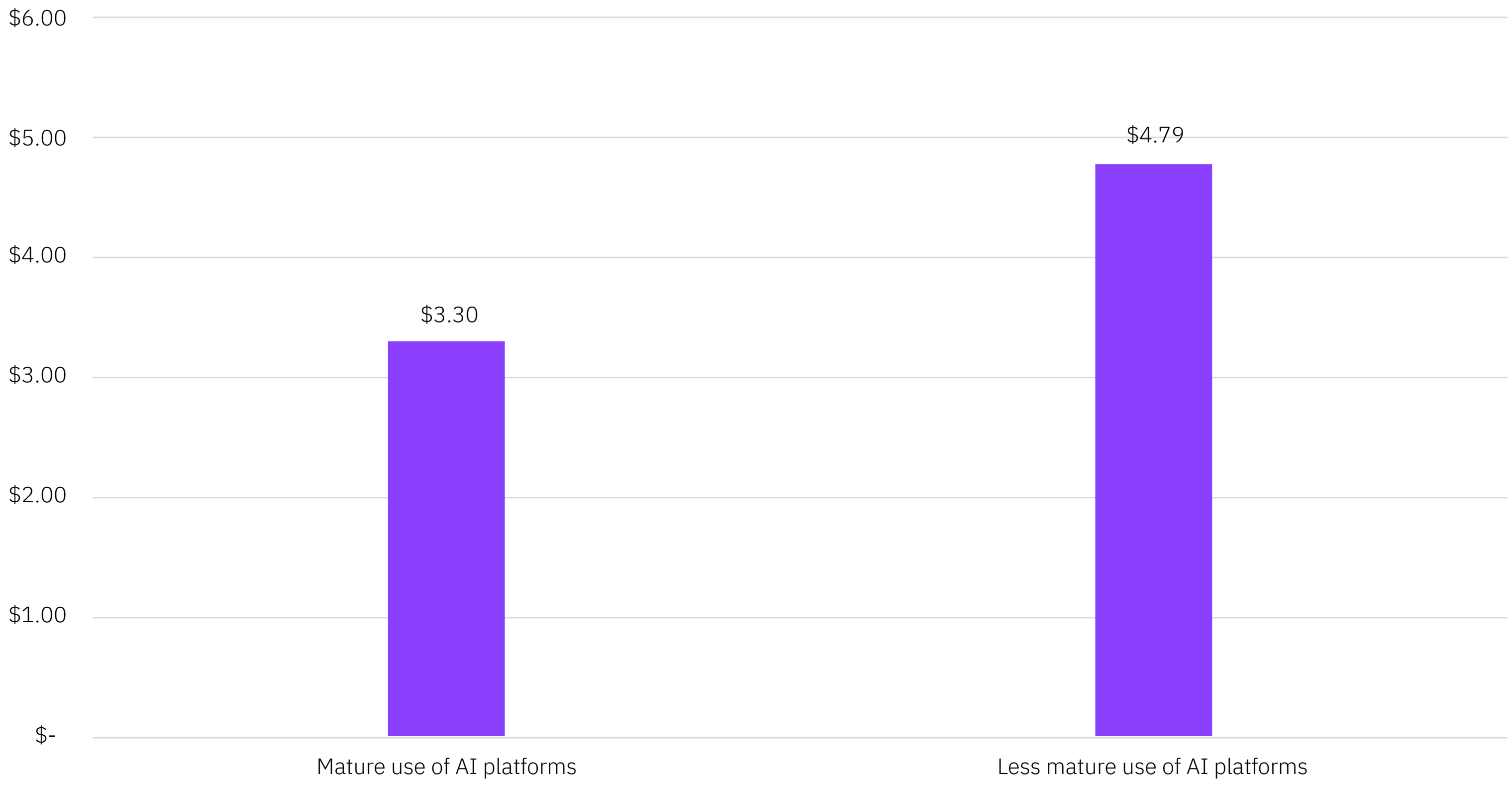


Figure 23

Impact of AI platforms on average cost of a data breach

Measured in US$ millions



Organizations with a mature use of AI platforms had a significantly lower average cost.

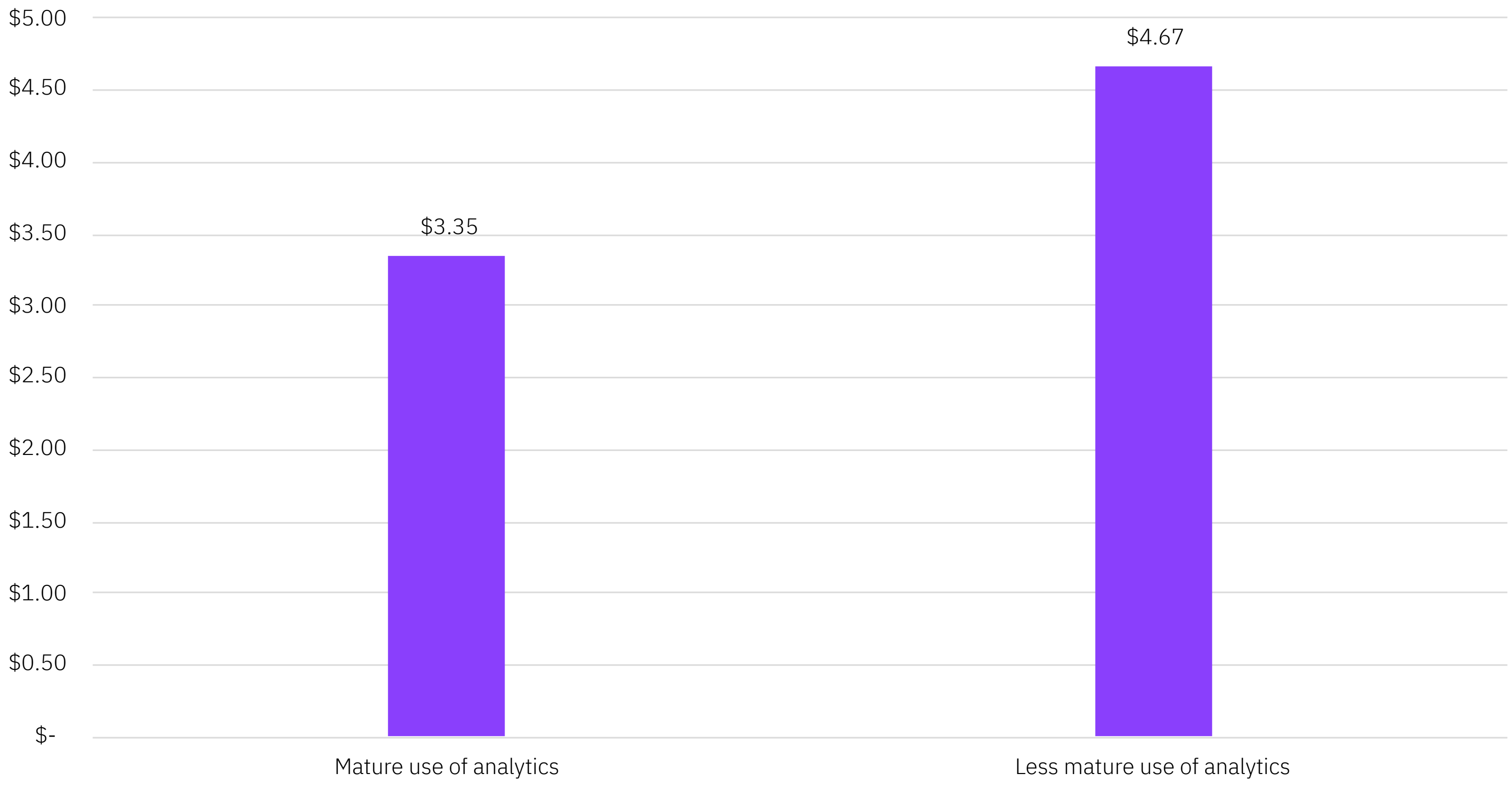
The average total cost of a data breach was $3.30 million at organizations with a more mature use of AI platforms (e.g., machine learning projects that cut across multiple tools).

At organizations with less mature use of AI platforms (e.g., just one application using machine learning), he average total cost was $1.49 million higher, a cost difference of 36.8%.

Figure 24

Impact of security analytics on average cost of a data breach

Measured in US$ millions



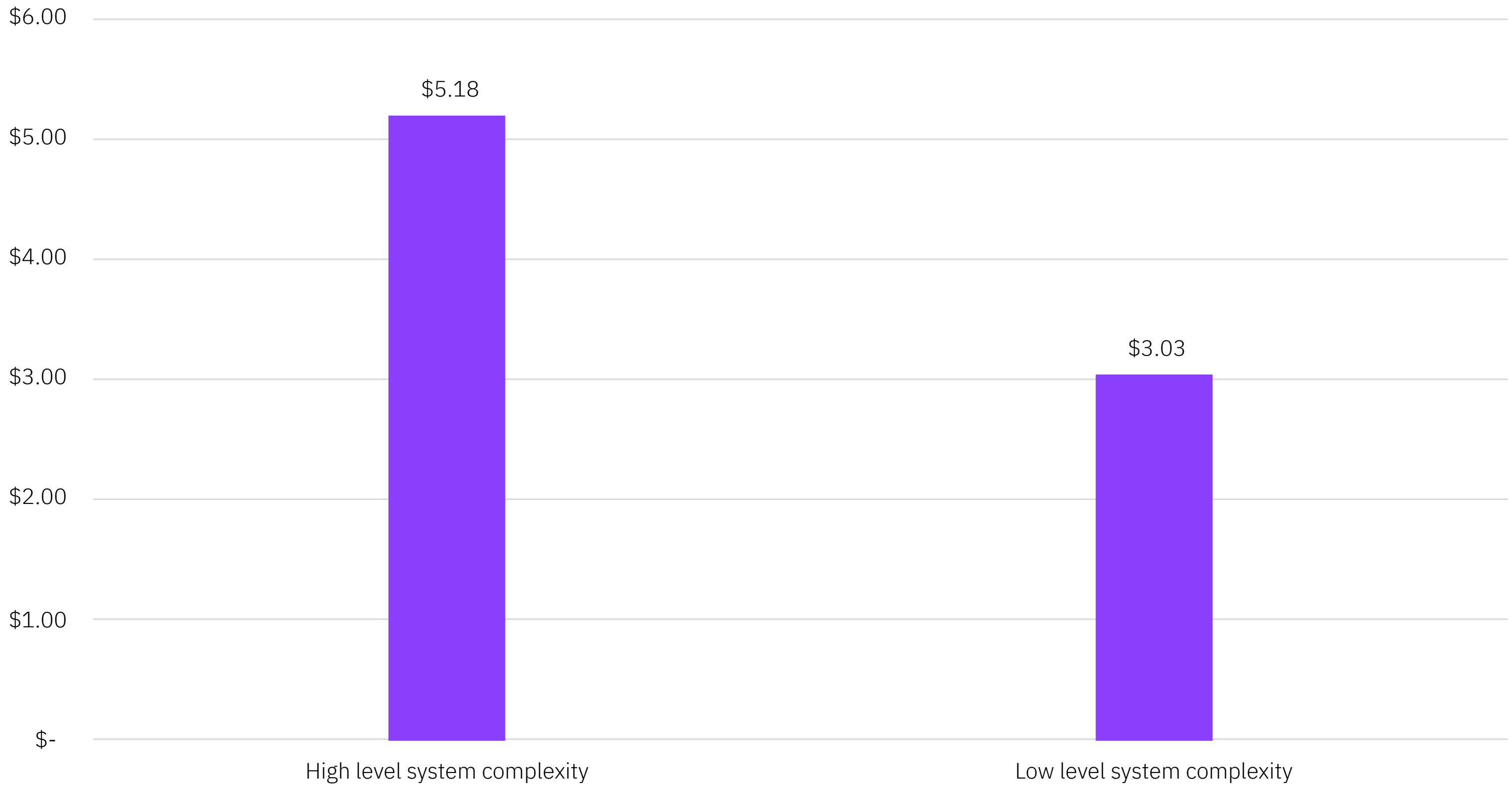
Mature use of analytics was associated with lower breach costs.

Organizations with a mature use of analytics had an average total cost of a breach of $3.35 million, compared to $4.67 million at organizations with a less mature use of analytics, a difference of $1.32 million or 32.9%.

Figure 25

Impact of system complexity on average cost of a data breach

Measured in US$ millions



System complexity was associated with higher breach costs.

Organizations with a high level of system complexity (e.g., a higher number of tools, systems, devices, data and users) had an average cost of a breach of $5.18 million, compared to $3.03 million at organizations with low levels of system complexity, for a difference of $2.15 million or 52.4%.

Cloud breaches and migration

This was the first year we took an extensive look at the effects of breaches in the cloud and the cost impact of cloud migration.

Key finding

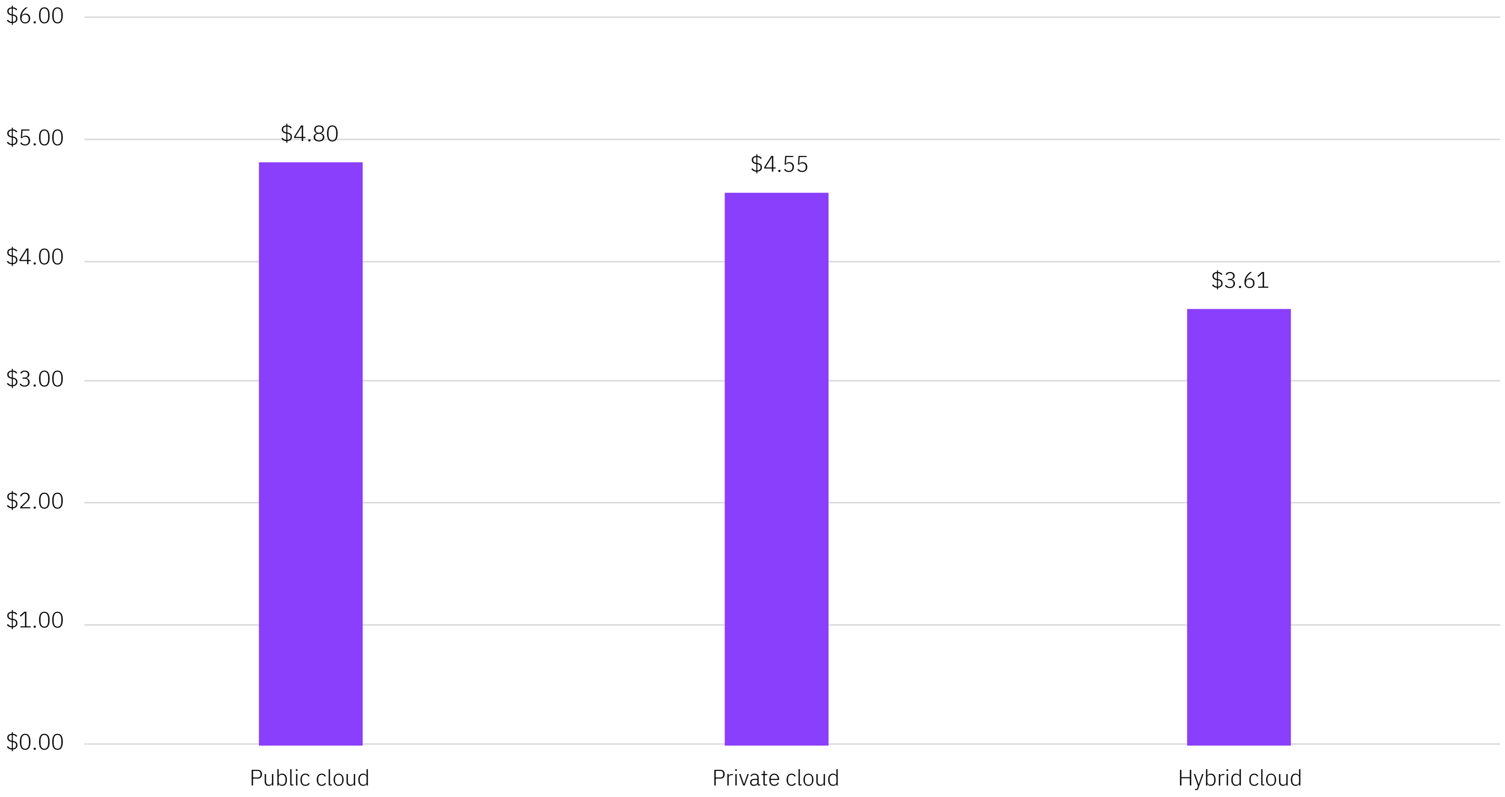
252 days

Average time to identify and contain a breach at organizations in mature stage of cloud modernization

Figure 26

Average total cost of a cloud-based breach by cloud model

Measured in US$ millions



The hybrid cloud model had the lowest average total cost of a data breach.

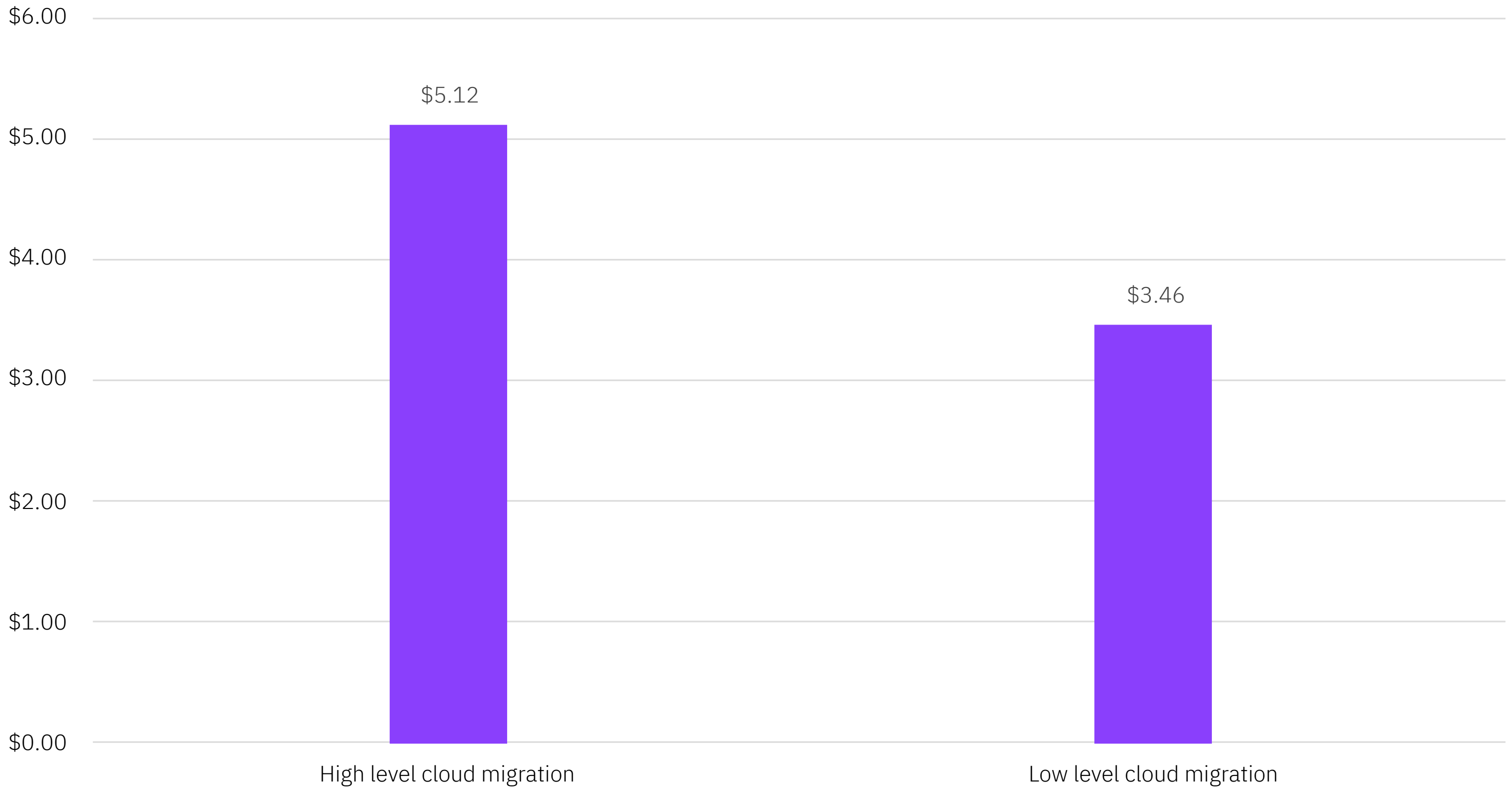
Public cloud breaches cost an average of $4.80 million compared to $4.55 million for breaches in private clouds, and $3.61 million for hybrid cloud breaches. Hybrid cloud breaches cost an average of $1.19 million less than public cloud breaches, or a difference in cost of 28.3%.

Public cloud = at least 80% conforming to the public cloud environment and no more than 20% conforming to hybrid cloud. Private cloud = at least 80% conforming to the private cloud environment and no more than 20% conforming to hybrid cloud.

Figure 27

Impact of cloud migration on average cost of a data breach

Measured in US$ millions



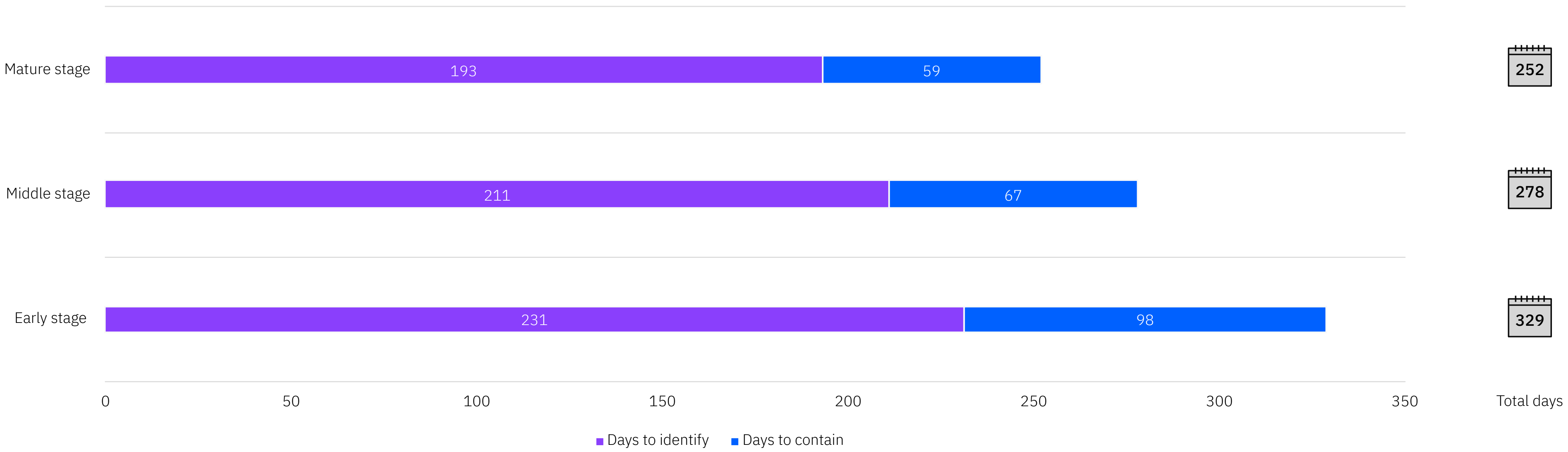
Extensive cloud migration was the third highest cost amplifying factor in a study of 25 cost factors.

Organizations with a high level of cloud migration had an average cost of a breach of $5.12 million, compared to $3.46 million for organizations with low levels of cloud migration, for a difference of $1.66 million or 38.7%.

Figure 28

Days to identify and contain a cloud-based data breach by cloud modernization stage

Measured in days



Cloud-based data breaches took longer on average to identify and contain among organizations in early stages of their overall cloud modernization journey, compared to those in middle and mature stages.

It took organizations an average of 231 days to identify and 98 days to contain a cloud-based breach in the early stage of cloud modernization (329 days total), compared to 193 days to identify and 59 days to contain a cloud breach in the mature stage of cloud modernization (252 days total). In the early stage of cloud modernization, it took an average of 42 days longer to identify and contain a breach than the global average time to identify and contain a breach (329 days vs. 287 days).

COVID-19 and remote work

This is the second year of this report that has been published during the pandemic. Last year, the pandemic began after most of the breaches in the study had already happened, so we re-surveyed organizations to get their predictions about how remote working due to COVID-19 would impact breach costs and the breach lifecycle. For this year's report we were able to assess the impacts of remote working on breaches that all occurred during the pandemic.

Key finding

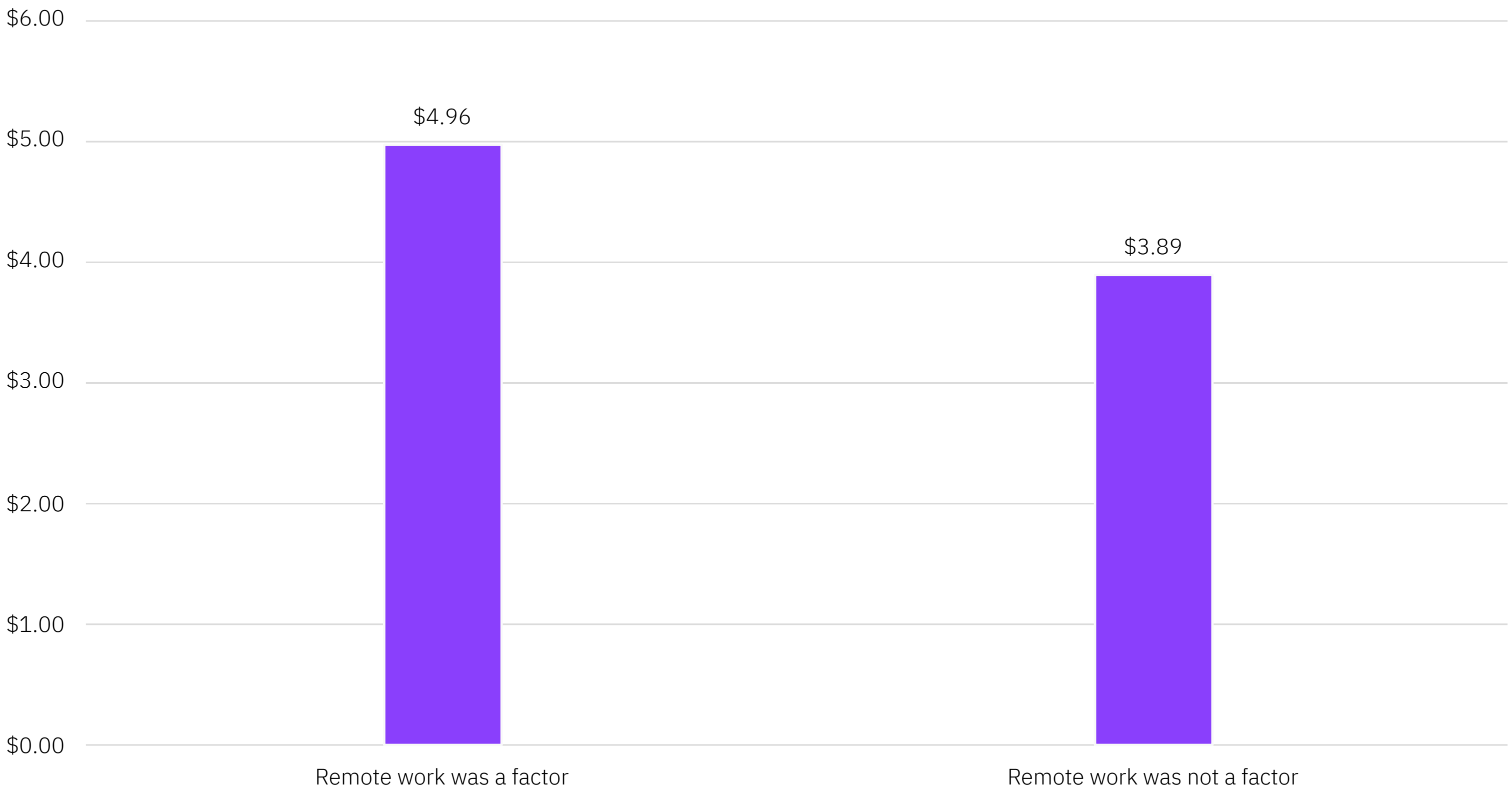
$5.54m

Average cost of a breach at organizations with 81-100% of employees working remotely

Figure 29

Average cost of a data breach where remote work was a factor

Measured in US$ millions



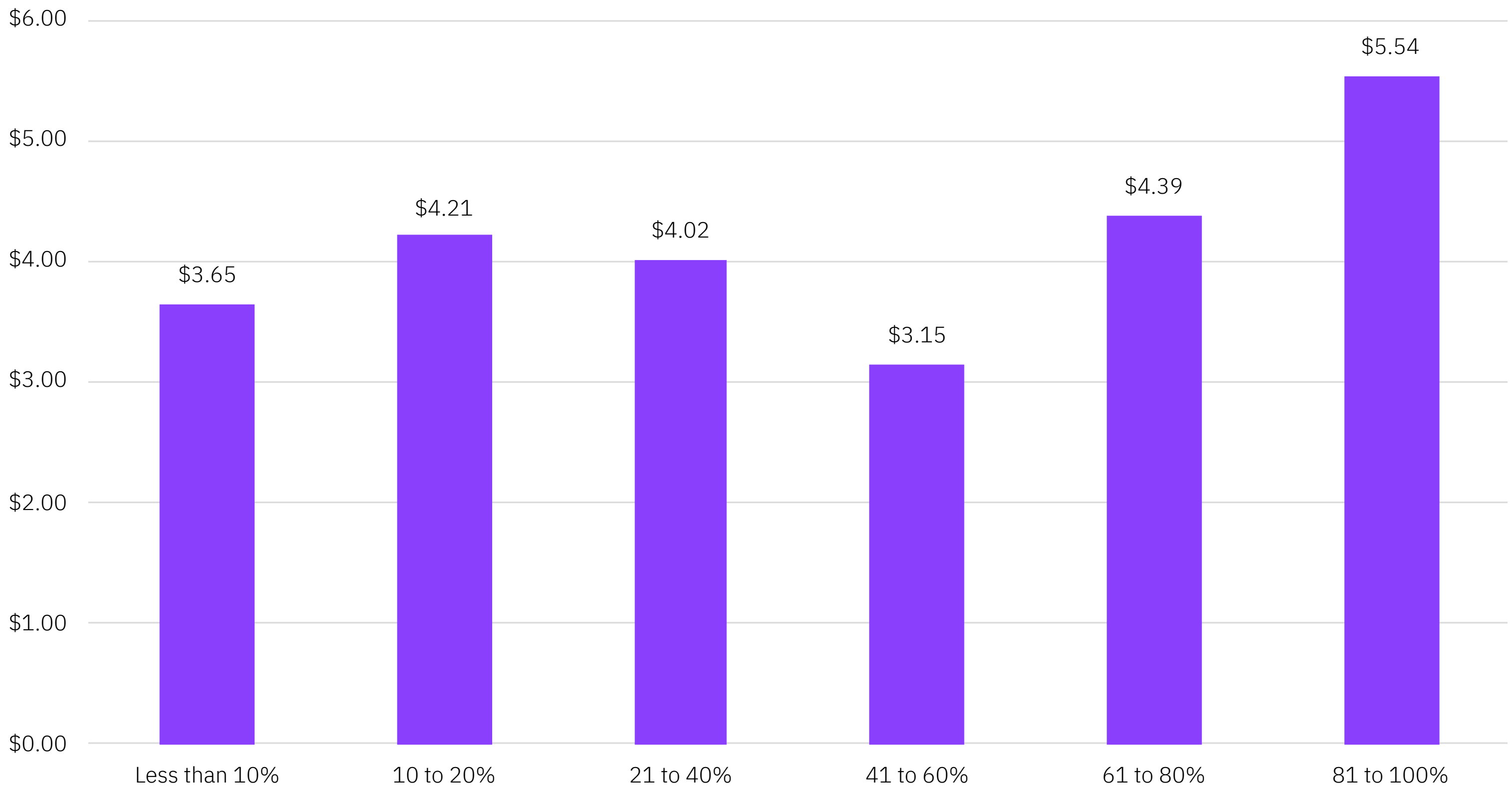
The average total cost of a data breach was more than $1 million higher where remote working was a factor in causing the breach compared to breaches where remote working was not a factor.

At organizations where remote work was a factor in the breach, the average total cost of a data breach was $4.96 million. When remote work was not a factor in causing the breach, the average total cost was $3.89 million. The difference in cost between breaches where remote work was a factor and where remote work was not a factor in the breach was $1.07 million, or 24.2%.

Figure 30

Average cost of a breach based on share of employees working remotely

Measured in US$ millions



Organizations where more than 60% of employees were working remotely, had an average cost of a data breach that was higher than the overall average cost of a breach.

For organizations with 61-80% of employees working remotely, the average cost was $4.39 million, or $0.15 million more than the overall average of $4.24 million. At organizations with 81-100% of employees working remotely, the average cost of a data breach was $5.54 million, or $1.30 million more than the overall average of $4.24 million, a cost difference of 26.6%.

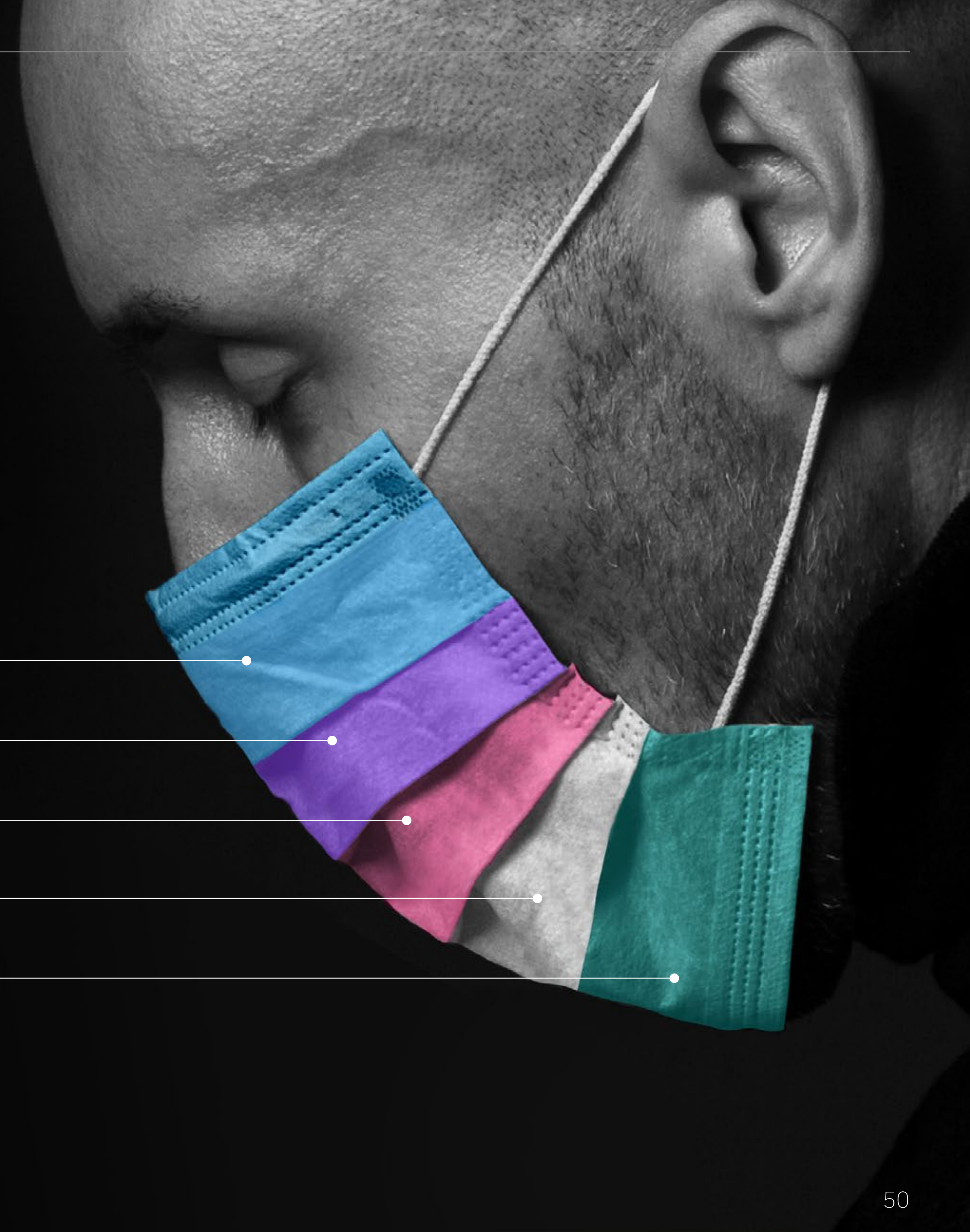
Figure 31

Average cost of a data breach based on level of digital transformation due to COVID-19

Measured in US$ millions

The cost of a breach was higher than average at organizations that had not undergone a digital transformation due to COVID-19.

When organizations made no effort at digital transformation (i.e., adapted their IT to cope with the pandemic) the average cost of a breach was $5.01 million, or $0.77 million more than the global overall average of $4.24 million.

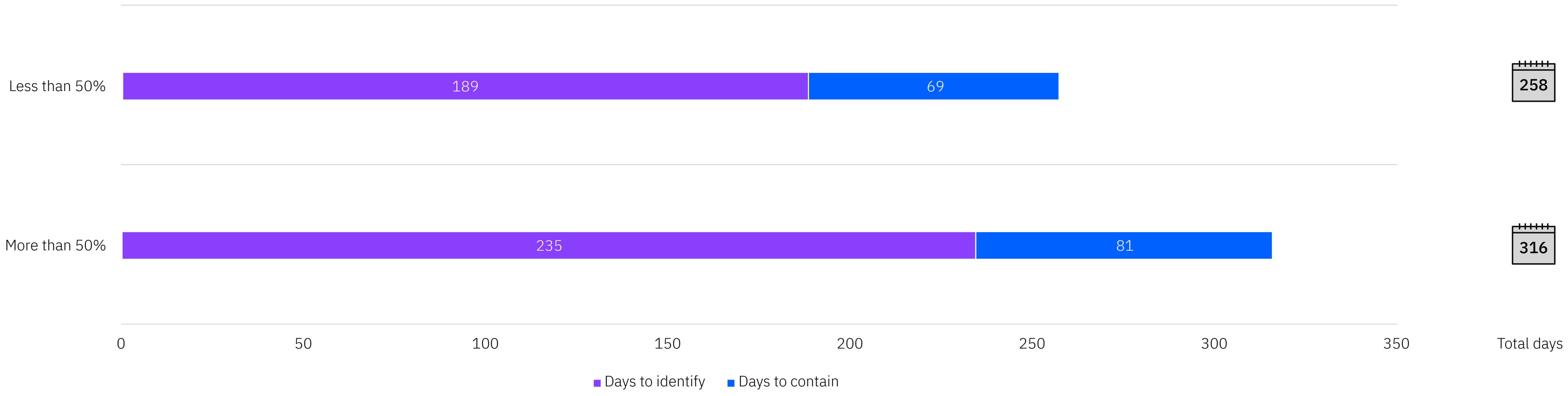


$5.01m No transformation
$4.13m Minimal transformation
$3.78m Moderate transformation
$3.97m Significant transformation
$4.26m Very significant transformation

Figure 32

Average time to identify and contain a breach based on level of remote work adoption

Measured in days



Organizations that had implemented remote work at greater than a 50% level experienced a longer than average time to identify and contain a data breach.

At organizations where remote work was at greater than 50% adoption, it took an average of 235 days to identify and 81 days to contain a breach (316 days total), compared to the overall average of 212 days to identify and 75 days to contain (287 days total), for a difference of 9.6%. With less than 50% remote work adoption, a data breach took an average of 189 days to identify and 69 days to contain (258 days total), a difference of 10.6%.

Cost of a mega breach

Mega breaches, those with more than 1 million compromised records, are not the normal experience for most businesses. But mega breaches have an outsized impact on consumers and industries. The average cost of a mega breach has continued to grow since we introduced this analysis in the 2018 study.

This year's investigation is based on the analysis of 14 companies that experienced a data breach involving the loss or theft of 1 million or more records. For a full explanation of our methodology, see the cost of a data breach FAQ at the end of this report.

Key finding

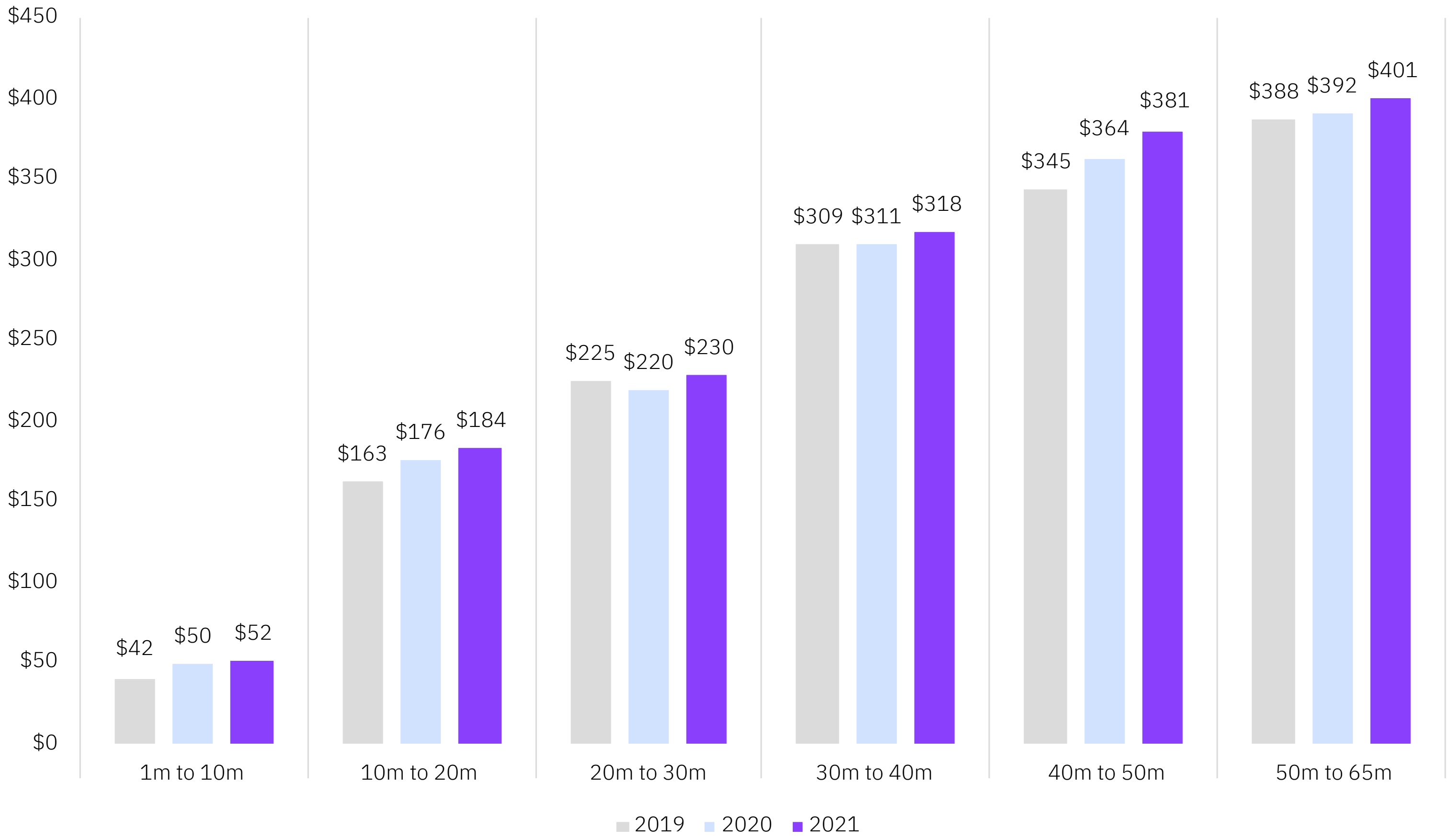
$401m

Average total cost for breaches of 50 million to 65 million records

Figure 33

Average total cost of a mega breach by number of records lost

Measured in US$ millions



The average cost of a mega breach was $401 million for the largest breaches (50 million to 65 million records), an increase from $392 million in 2020.

This represents an increase of 2.3%. The cost increased across all subsets of the mega breaches (1 million up to 65 million records). The largest cost increase was in the 40 million to 50 million records range, from $364 million in 2020 to $381 million in 2021, an increase of 4.7%. In the range of 1 million to 10 million records, costs increased 4% year over year and have increase by 23.8% since the 2019 report.

Quantifying security risk

Security is a business problem. Board executives and business leaders want to know the likelihood of a cyber incident occurring and the impact to the company's ability to produce and sell its products or services as well as the potential impact to the brand.

Risk quantification can help organizations identify and prioritize security risk to inform decisions such as deploying new technologies, making investments in their business, and changing processes. CISOs, risk managers and security teams can use benchmark research like the Cost of a Data Breach Report to infer general trends and cost averages in their industry or geography.

However, using data specific to the organization, rather than industry averages, organizations can get clarity and understanding on potential security gaps and how to reduce overall risk by quantifying security risk into financial terms.

Below we explain how the Factor Analysis of Information Risk (FAIR), an open international standard for cyber risk modeling, combined with threat intelligence, can help organizations assess the potential impacts of cyber risks through financial projections and probabilities.

Case study

How IBM Security uses FAIR in risk modeling

To quantify risk specific to your organization, IBM Security uses the FAIR model to estimate the probability of a data breach and size of the breach in financial terms. We look at variables such as frequency of breach events, vulnerabilities and strength of security.

We then use threat intelligence from IBM Security X-Force to assess the capability of the threat actor and their probability to attack.

We take these variables through statistical analysis using Monte Carlo Simulations to estimate the range of financial loss. Understanding these key variables allows an organization to identify gaps in current controls or processes that put them at risk for larger financial loss.

We can define the material impact of security gaps into components of primary and secondary loss; with primary loss being the loss associated with managing and responding to the event and secondary loss being the loss associated with outside parties such as regulatory bodies, customers and the stock market.

Once we understand the potential financial loss an organization faces, we can look at cost-benefit and ROI analysis into possible investments around mitigating controls or processes. For example, improvements around security awareness training can help to reduce threat event frequency, or changes to the identity and access management program can help minimize the size of a breach.

Data from the IBM X-Force Threat Intelligence Index shows us that the banking and financial services industry is a highly targeted sector of business year after year. In this example, we look at a hypothetical loss event in financial services.

Scenario

Financial services sensitive data breach

This hypothetical scenario analyzes the risk associated with a malicious external actor gaining access to a sensitive database and using ransomware to halt operations and extort the organization by threatening to expose stolen data publicly.

In a real-world client engagement, our assumptions, which serve as data inputs for our analysis, are gathered via consultative workshops. In this scenario, we use financial industry averages and learnings from previous client engagements as inputs to run the statistical analysis.

Scope

Threat	Threat type	Method category	Asset	Loss effect
External actor(s)	Malicious	Ransomware	Database containing PII and PCI data	Loss of confidentiality

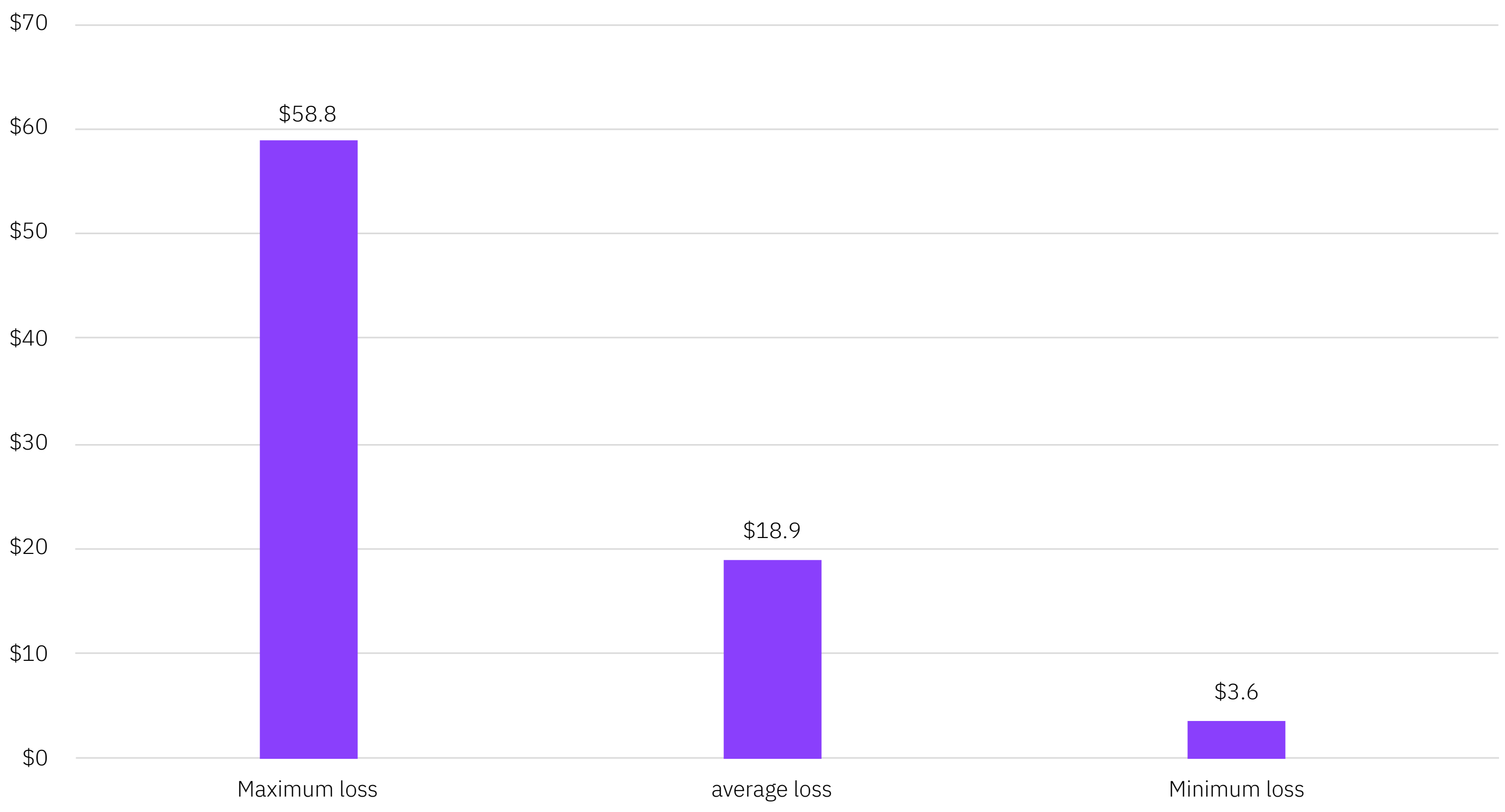
Assumptions

Threat event frequency	
2-4 times per year	Based on the current contact frequency, phishing and spam attempts and controls in place.
Vulnerability	
5% - 15%	Based on the strength of security controls and threat actor capability. The assumption is the controls are strong against this specific type of threat.
Direct loss	
Response time to manage the event - Person hours	
50 - 150 hours	Based on the size of the loss
Employee wages based on skill level needed to repair and restore	
$75 - $150 per hour	Based on skill level required for specific response
Secondary loss to customers	
Sensitive Records	
500,000 to 1M 75 - 100% PII/PCI 10 - 25% IP	Estimated database of sensitive records Estimated percentage that contain PCI or PII Estimated percentage that contain IP

Figure 34

Range of financial loss

Measured in US$ millions

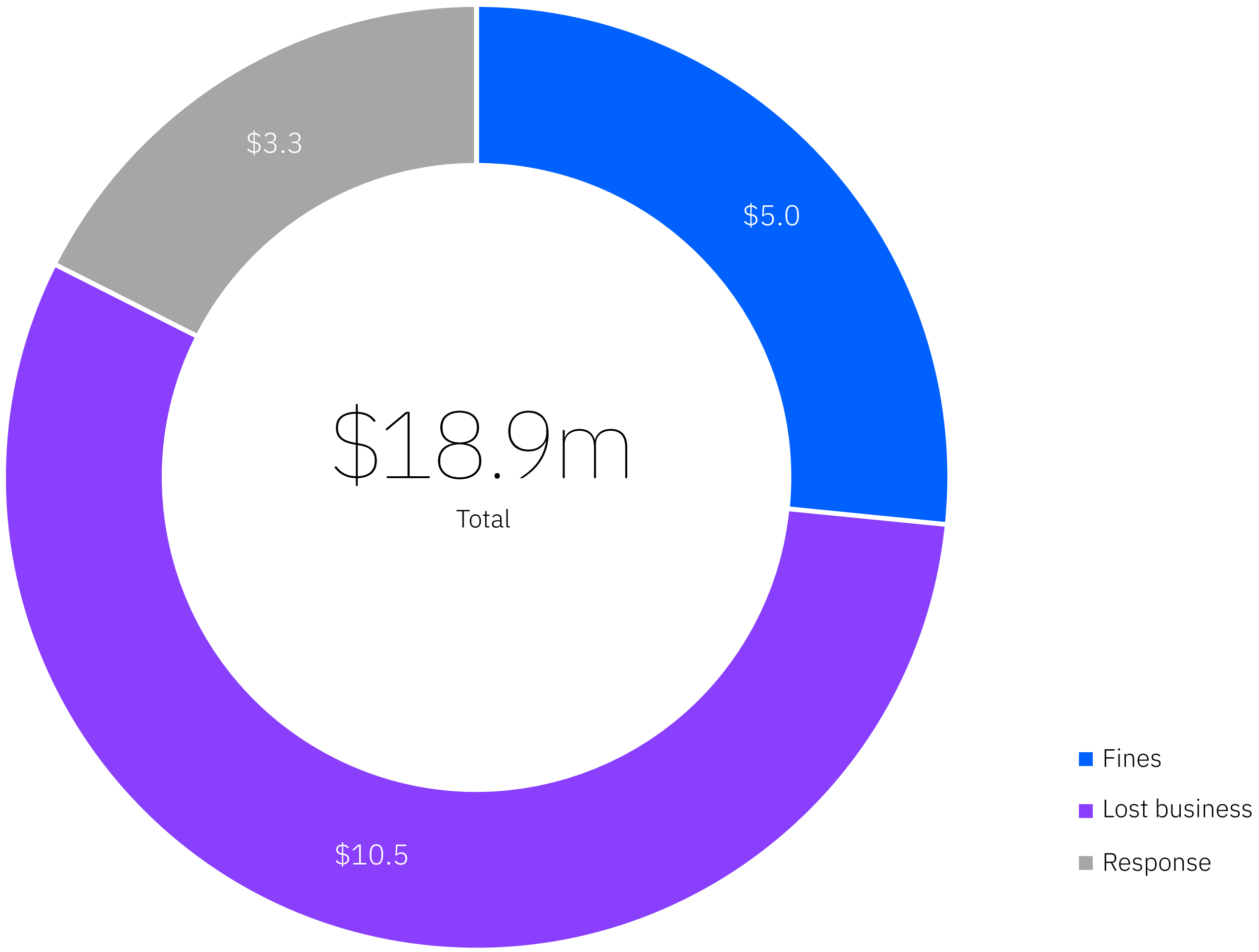


Quantifying the security risk of a specific bank being hit by ransomware, shows a 30% probability of the event occurring given that bank's strong security controls and an $18.9 million average financial loss that is composed of response costs, lost business and regulatory fines.

Figure 35

Components of financial loss

Measured in US$ millions



Largest primary form of loss

Response costs

Largest secondary form of loss

Lost business

Most severe event

$18.9 million

Probability of loss exceeding $1 million

30%

Top annualized risk

$5.7 million

Recommendations to help minimize financial impacts of a data breach

Invest in security orchestration, automation and response (SOAR) to help improve detection and response times.

In the cost of a data breach study, security AI and automation significantly reduced the average time to identify and respond to a data breach had a lower average cost. SOAR and SIEM software, and managed detection and response and services, can help your organization accelerate incident response with automation, process standardization and integration with your existing security tools. Automation technologies including artificial intelligence, analytics and automated orchestration were all associated with lower than average data breach costs.

Adopt a zero trust security model to help prevent unauthorized access to sensitive data.

Results from the study showed that just 35% of organizations had implemented a zero trust security approach. However, those in the mature stage of their zero trust deployment had an average breach cost that was $1.76 million less than organizations without zero trust. As organizations have shifted to incorporate remote work and more disconnected, hybrid multicloud environments, a zero trust strategy can help protect data and resources by making them accessible only on a limited basis and in the right context.

Stress test your incident response plan to increase cyber resilience.

Organizations in the study who have formed incident response (IR) teams and tested their incident response plans saw an average total cost of a data breach that was $2.46 million less than organizations that experienced a breach without an IR team or a tested IR plan. The mantra "train like you fight and fight like you train" means developing and testing incident response playbooks to help optimize your ability to respond quickly and effectively to attacks.

Use tools that help protect and monitor endpoints and remote employees.

In the study, organizations that had more than 60% of their employees working remotely in response to the COVID-19 pandemic had a higher than average cost of a data breach. Unified endpoint management (UEM) and identity and access management (IAM) products and services can help provide security teams with deeper visibility into suspicious activity on company and bring your own (BYO) laptops, desktops, tablets, mobile devices and IoT, including endpoints the organization doesn't have physical access to, speeding investigation and response time to isolate and contain the damage.

Invest in governance, risk management and compliance programs.

An internal framework for audits, evaluating risk across the enterprise and tracking compliance with governance requirements can help improve an organization's ability to detect a data breach and escalate containment efforts. The FAIR risk quantification methodology can help ascertain the probability of security incidents and calculate the associated costs in business value. Quantifying the cost of a potential breach can help in the decision-making process for allocating resources.

Embrace an open security architecture and minimize the complexity of IT and security environments.

In this year's study, complexity of IT and security systems and extensive cloud migration were among the top factors contributing to higher average data breach costs. Security tools with the ability to share data between disparate systems can help security teams detect incidents across complex hybrid multicloud environments. A managed security services provider can also help simplify security and risk with continuous monitoring and integrated solutions and services.

Protect sensitive data in cloud environments using policy and encryption.

With the increasing amount and value of data being hosted in cloud environments, organizations should take steps to protect cloud-hosted databases. Use data classification schema and retention programs to help bring visibility into and reduce the volume of the sensitive information that is vulnerable to a breach, and protect it using data encryption and fully homomorphic encryption. Use vulnerability scanning, penetration testing and red teaming to help identify cloud-hosted database vulnerability exposures and misconfigurations.

Recommendations for security practices are for educational purposes and do not guarantee results.

Organization characteristics

This section shows the breakdown of organizations in the study by geography and industry. It includes definitions used for classifying the organizations by industry, and data on the average cost of a data breach by organization size.

Figure 36

Distribution of the sample by geography

This year's study included 537 organizations of various sizes, sampled across a wide range of geographies and industries. The 2021 study was conducted in 17 countries or regional samples and 17 industries.

Countries	17
Organizations	537
Contribution to study	%

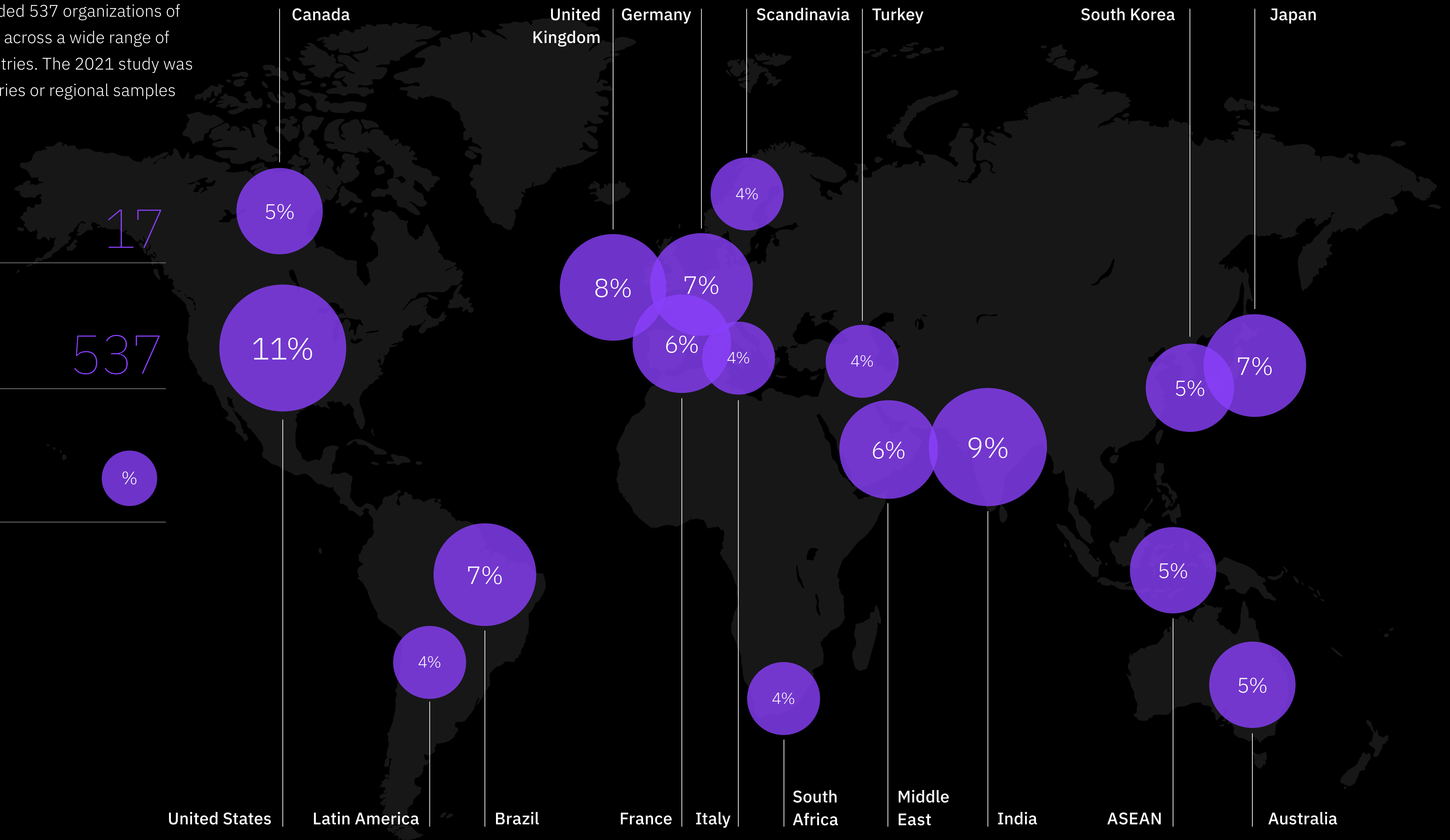
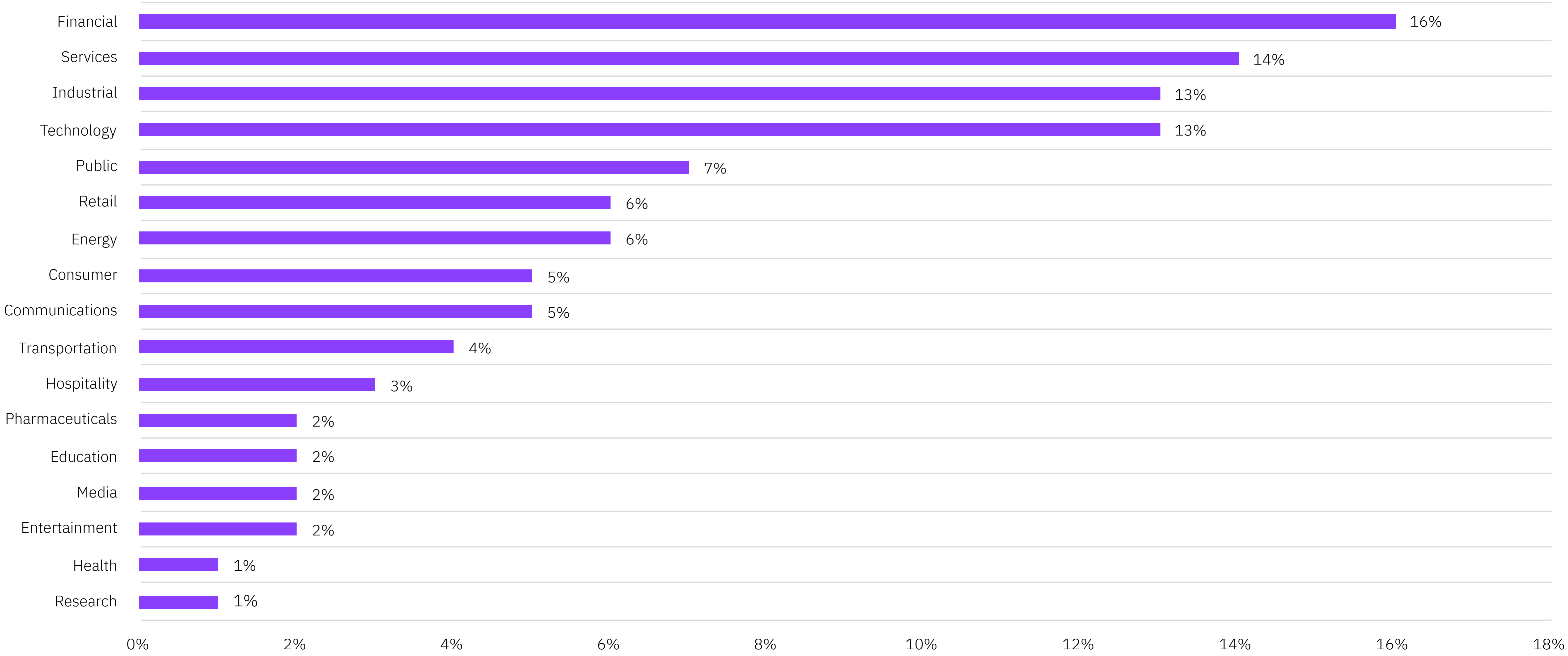


Figure 37

Distribution of the sample by industry



Industry definitions

Healthcare
Hospitals, clinics

Financial
Banking, insurance, investment companies

Energy
Oil and gas companies, utilities, alternative energy producers and suppliers

Pharmaceuticals
Pharmaceutical, including biomedical life sciences

Industrial
Chemical process, engineering and manufacturing companies

Technology
Software and hardware companies

Education
Public and private universities and colleges, training and development companies

Services
Professional services such as legal, accounting and consulting firms

Entertainment
Movie production, sports, gaming and casinos

Transportation
Airlines, railroad, trucking and delivery companies

Communication
Newspapers, book publishers, public relations and advertising agencies

Consumer
Manufacturers and distributors of consumer products

Media
Television, satellite, social media, Internet

Hospitality
Hotels, restaurant chains, cruise lines

Retail
Brick and mortar and e-commerce

Research
Market research, think tanks, R&D

Public
Federal, state and local government agencies and NGOs

Impact of organization size

The Cost of a Data Breach report drew on 537 organizations across small, medium and large-sized organizations. In this analysis of the impact of organization size, we examined the cost by employee headcount, which is a proxy for size.

Key finding

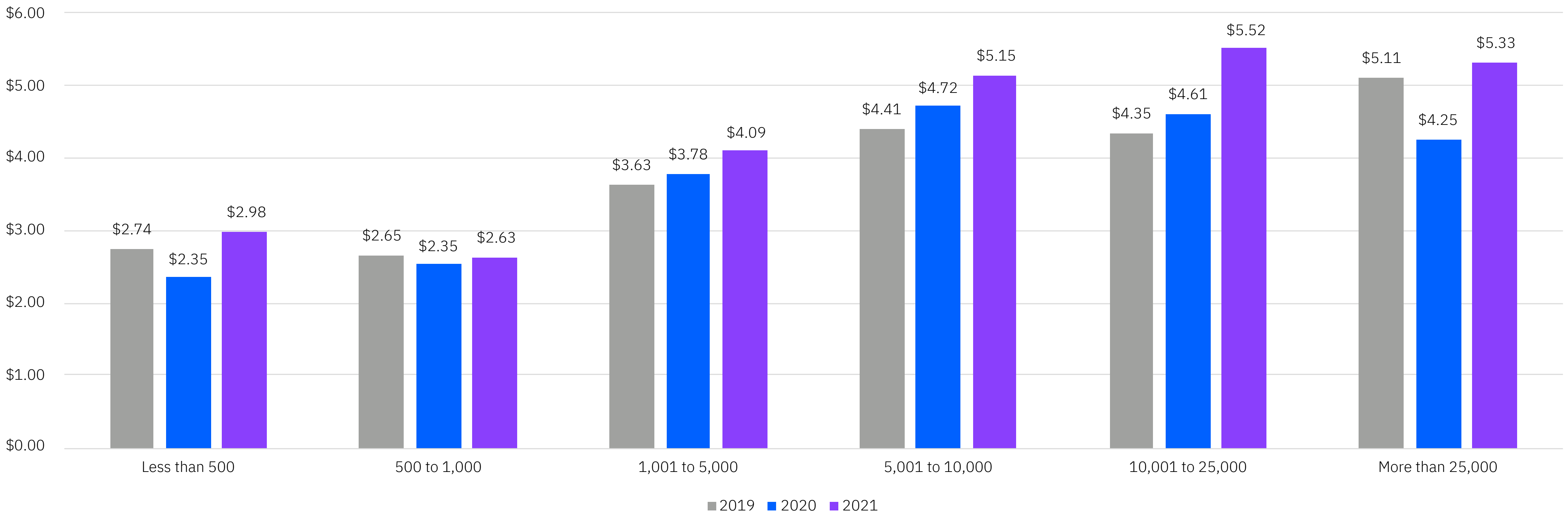
$5.33m

Average total cost of a breach at organizations with over 25,000 employees

Figure 38

Average cost of a data breach by employee headcount

Measured in US$ millions



Bigger organizations had the biggest data breach costs.

By organizational size, the costliest size was 10,000-25,000 employees, at an average total cost of $5.52 million, followed by more than 25,000 employees at $5.33 million. Small businesses (less than 500 employees) saw an increase from 2.35 million in 2020 to $2.98 million in 2021, a 26.8% increase. The study represented organizations rather evenly across different sizes: 25% of organizations had less than 1,000 employees; 20% had from 1,001-5,000 employees; 22% had 5,001-10,000 employees; 15% had from 10,001-25,000 employees; and 18% had more than 25,000 employees.

Research methodology

To preserve confidentiality, the benchmark instrument did not capture any company-specific information. Data collection methods did not include actual accounting information but instead relied upon participants estimating direct costs by marking a range variable on a number line. Participants were instructed to mark the number line in one spot between the lower and upper limits of a range for each cost category.

The numerical value obtained from the number line, rather than a point estimate for each presented cost category, preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

To ensure a manageable size for the benchmarking process, we carefully limited items to only those cost activity centers that we considered crucial to data breach cost measurement. Based upon discussions with experts, the final set of items included a fixed set of cost activities. Upon collection of the benchmark information, each instrument was re-examined carefully for consistency and completeness.

The scope of data breach cost items contained within our benchmark instrument was limited to known cost categories that applied to a broad set of business operations that handle personal information.

We believed that a study focused on business process — and not data protection or privacy compliance activities — would yield better quality results.

Data breach FAQ

What is a data breach?
A breach is defined as an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk — either in electronic or paper format. Breaches included in the study ranged from 2,000 to 101,000 compromised records.

What is a compromised record?
A record is information that identifies the natural person (individual) whose information has been lost or stolen in a data breach. Examples include a database with an individual's name, credit card information and other personally identifiable information (PII) or a health record with the policyholder's name and payment information.

How do you collect the data?
Our researchers collected in-depth qualitative data through nearly 3,500 separate interviews with individuals at 537 organizations that suffered a data breach between May 2020 and March 2021. Interviewees included IT, compliance and information security practitioners who are knowledgeable about their organization's data breach and the costs associated with resolving the breach. For privacy purposes, we did not collect organization-specific information.

How do you calculate the cost?
To calculate the average cost of a data breach, we collected both the direct and indirect expenses incurred by the organization. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates. Only events directly relevant to the data breach experience are represented in this research. For example, new regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) may encourage organizations to increase investments in their cybersecurity governance technologies, but do not directly affect the cost of a data breach as presented in this research. For consistency with prior years, we use the same currency translation method rather than adjusting accounting costs.

How does benchmark research differ from survey research?
The unit of analysis in the Cost of a Data Breach Report is the organization. In survey research, the unit of analysis is the individual. We recruited 537 organizations to participate in this study.

Can the average per record cost be used to calculate the cost of breaches involving millions of lost or stolen records?
The average cost of data breaches in our research does not apply to catastrophic or mega data breaches, such as Equifax, Capital One or Facebook. These are not typical of the breaches many organizations experience. Hence, to draw useful conclusions in understanding data breach cost behaviors, we target data breach incidents that do not exceed 100,000 records.

It is not consistent with this research to use the per record cost to calculate the cost of single or multiple breaches totaling millions of records. However, the study uses a simulation framework for measuring the cost impact of a "mega breach" involving 1 million or more records, based on a sample of 14 very large breaches of this size.

Why are you using simulation methods to estimate the cost of a mega data breach?
The sample size of 14 companies experiencing a mega breach is too small to perform a statistically significant analysis using activity-based cost methods. To remedy this issue, we deploy Monte Carlo simulation to estimate a range of possible (random) outcomes through repeated trials. In total, we performed more than 150,000 trials. The grand mean of all sample means provides a most likely outcome at each size of data breach – ranging from 1 million to 65 million compromised records.

Are you tracking the same organizations each year?
Each annual study involves a different sample of companies. To be consistent with previous reports, we recruit and match companies each year with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach. Since starting this research in 2005, we have studied the data breach experiences of 4,477 organizations.

Research limitations

Our study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations with this benchmark research that need to be carefully considered before drawing conclusions from findings.

Non-statistical results
Our study draws upon a representative, non-statistical sample of global entities. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.

Non-response
Non-response bias was not tested, so it is possible that companies that did not participate are substantially different in terms of underlying data breach cost.

Sampling-frame bias
Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.

Company-specific information
The benchmark does not capture company-identifying information. It allows individuals to use categorical response variables to disclose demographic information about the company and industry category.

Unmeasured factors
We omitted variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined.

Extrapolated cost results
While certain checks and balances can be incorporated into the benchmark process, it is always possible that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

Extrapolated cost results
This year, a strong U.S. dollar significantly influenced the global cost analysis. The conversion from local currencies to the U.S. dollar deflated the per record and average total cost estimates. For purposes of consistency with prior years, we decided to continue to use the same accounting method rather than adjust the cost.

About Ponemon Institute and IBM Security

The Cost of a Data Breach Report is produced jointly between Ponemon Institute and IBM Security. The research is conducted independently by Ponemon Institute, and the results are sponsored, analyzed, reported and published by IBM Security.

Ponemon INSTITUTE

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government.

Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

Ponemon Institute upholds strict data confidentiality, privacy and ethical research standards, and does not collect any personally identifiable information from individuals (or company identifiable information in business research). Furthermore, strict quality standards ensure that subjects are not asked extraneous, irrelevant or improper questions.

IBM **Security**

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than 4.7 trillion events per month in more than 130 countries, IBM holds over 10,000 security patents. To learn more, visit ibm.com/security.

Contact us on Twitter at @IBMSecurity. Join the conversation in the IBM Security Community.

If you have questions or comments about this research report, including for permission to cite or reproduce the report, please contact by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City
Michigan 49686 USA

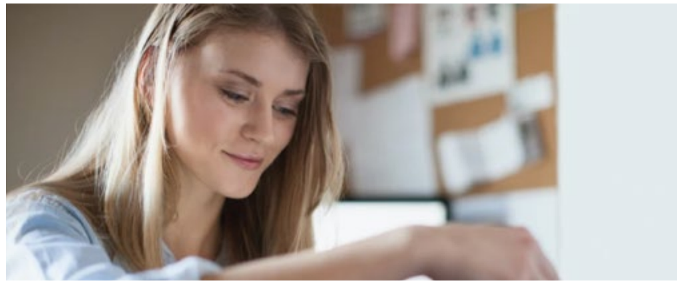
1.800.887.3118
research@ponemon.org

Take the next steps

Cybersecurity services

Reduce risk with consulting,
cloud and managed security services

Learn more →



Identity and access management

Connect every user, API and device
to every app securely

Learn more →

Data security

Discover, classify and protect
sensitive enterprise data

Learn more →

Security information and event management

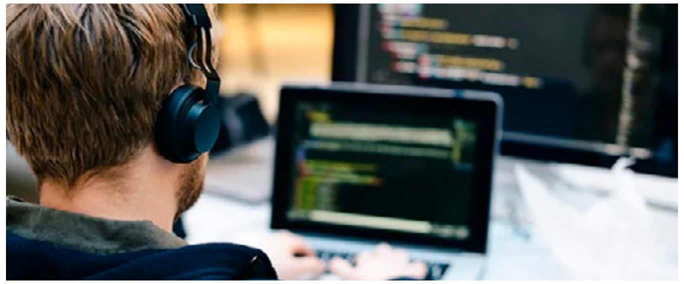
Gain visibility to detect, investigate and
respond to threats

Learn more →

Security orchestration, automation and response

Accelerate incident response with orchestration and automation

Learn more →



Cloud security

Integrate security into your journey to hybrid multicloud

Learn more →

Zero Trust

Wrap security around every user, device and connection

Learn more →

IBM **Security**

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2021

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

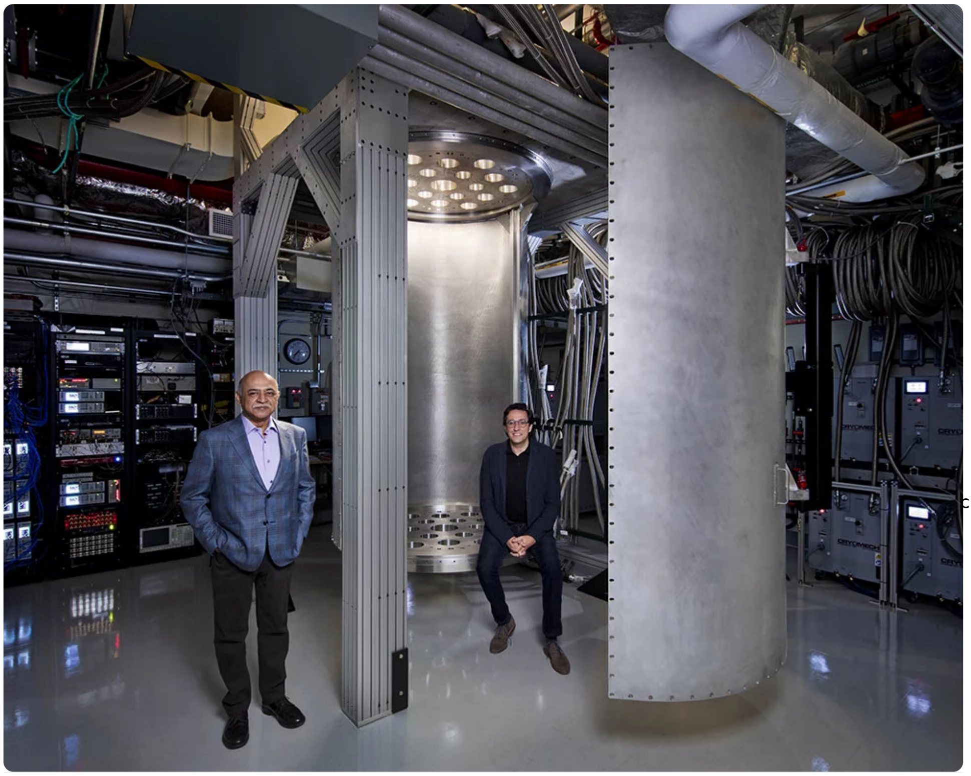
IBM products are warranted according to the terms and conditions of the agreements under which they are provided. The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

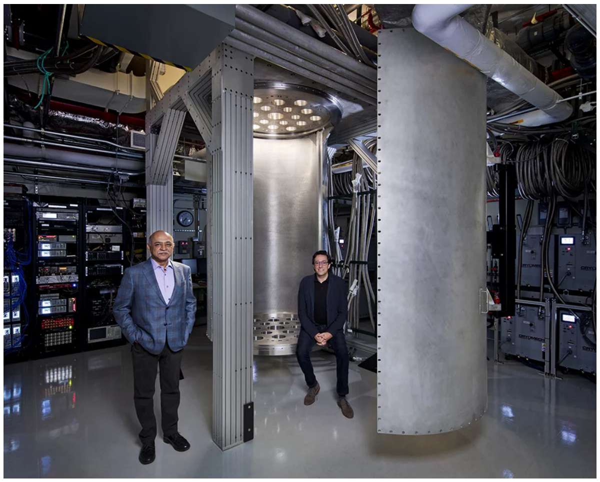
/company/the-quantum-daily/)
m/QuantumDaily)
UClbf-5iPFjQ-LY3RyfQyng/featured)
m.com/thequantuminsider)
Quantum-Insider-105937977453873/)
m/@thequantuminsider)

Nev
Quantum Comp
Natic
Resea
Capital M
Exclus
Insig
Educa
Interv
Mec
Repc
Abou
Intellig
Marke
Jok
CONTACT US(HTTPS://WWW.THEQUAI
SUBSC
METAVERSE INSIDER(HTTPS://
GUEST
(HTTPS://WWW.THEQUANTUMIN

IBM Research Reports Receiving More than 9,130 Patents in 2020, Quantum Computing "Getting Ever Better"

BY MATT SWAYNE(HTTPS://THEQUANTUMINSIDER.COM/AUTHOR/MATT-SWAYNE/)
JANUARY 12, 2021(HTTPS://THEQUANTUMINSIDER.COM/2021/01/12/)
QUANTUM COMPUTING BUSINESS (HTTPS://THEQUANTUMINSIDER.COM/CATEGORY/DAILY/BUSINESS/), RESEARCH (HTTPS://THEQUANTUMINSIDER.COM/CATEGORY/DAILY/RESEARCHANDTECH/)





IBM researchers received 9,130 patents in 2020. Quantum computing is a growing area in intellectual property development, the company indicates.

IBM researchers have cranked out more than 9,130 patents in 2020, many of them in deep tech areas, such as AI, cloud computing and quantum computing, according to a blog post (https://www.ibm.com/blogs/research/2021/01/ibm-patent-leadership-2020/).

The number places the company a unique global leadership position, according to the post.

"For me, this patent leadership symbolizes much more than just the mere fact of being at the top. A patent is evidence of an invention, protecting it through legal documentation, and importantly, published for all to read," writes Dario Gil (https://www.ibm.com/blogs/research/author/dariogil/), director of IBM Research (https://www.research.ibm.com/). "The number of patents we produce each year — and in 2020, it was more than 9,130 US patents — demonstrates our continuous, never-ending commitment to research and innovation. We are actively planting the research seeds of the bleeding edge technological world of tomorrow. Our most recent patents span artificial intelligence (AI), hybrid cloud, cyber-security and quantum computing. It doesn't get more future-looking than this."

Gil spotlights quantum computing, adding that this area is increasingly becoming a driver of IBM research and development.

"This next-generation technology is getting ever better," he writes "I am convinced that in the near future, products relying on quantum computation will be an integral part of our daily lives. By inventing and patenting those products today, we are ensuring our quantum future."

One of IBM's patents in quantum computing covers running molecular simulations on a quantum computer.

"Performing such simulations faster and across a much wider molecular space than a classical computer can ever do could help us design new molecules for novel drugs or catalysts," Gil Writes. "Another patent addresses the use of quantum computing in finance, to run risk analysis more precisely and efficiently than ever before."

Other patents are designed to help quantum computers perform better, according to the IBM research leader.

"Quantum computers of today are 'noisy' — meaning that the quantum bits, or qubits, they rely on get easily affected by any external disturbances," Gil added. "Many of our patents detail ways to make qubits much more stable and even suggest approached to correct the remaining errors in future stable qubits, the path to realize quantum error-correction and unleash the power of quantum computers to solve the currently unsolvable."

Big Blue, Deep Tech

Other deep technology areas covered by the patents include AI and the cloud. In cloud computing, the company received around 3,000 patents. about 2,300 AI patents.

"In cyber-security, I'd like to single out patents in fully homomorphic encryption — an area of cryptography where computations are made on data that stays encrypted at all times," writes Gil "With so many data leaks jeopardizing the privacy of our medical, genomic, financial and other sensitive records, secure encryption is more important than ever."

According to Gil, the company received about 3,000 patents, many focusing on data processing categorizations that can help bring services to the edge.

"In cyber-security, I'd like to single out patents in fully homomorphic encryption — an area of cryptography where computations are made on data that stays encrypted at all times," Gil writes. "With so many data leaks jeopardizing the privacy of our medical, genomic, financial and other sensitive records, secure encryption is more important than ever."

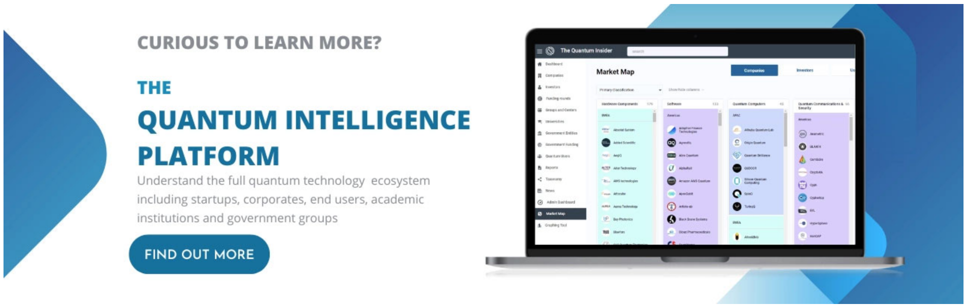
In AI, the company's researchers produced about 2,300 patents. Gil spotlights two ideas in his blog post.

"To take two examples among many: a novel way to search multilingual documents using natural language processing, and an ultra-efficient system for transferring image data taken by an on-vehicle camera," said Gil. "These both speak to the innovation and original thinking from our inventors in AI."

It Takes Time, But Patents Boost Innovation

Critics may charge that patent awards don't necessarily lead to practical solutions for people. Gil disagrees.

"One might argue against having patents that don't get immediately turned into commercial products," writes Gil. "But I disagree. Inventing something new is similar to putting forward a well thought out theory that may, one day, be verified experimentally. Perhaps not straight away, but it's still vital to have theories to enhance our overall understanding of a field and to keep progress going. Having future-looking patents is just as important as those aimed at products of today, and a broad portfolio of scientific advances always ends of up contributing to waves of innovation."


CURIOUS TO LEARN MORE?
THE
QUANTUM INTELLIGENCE
PLATFORM
Understand the full quantum technology ecosystem including startups, corporates, end users, academic institutions and government groups
FIND OUT MORE
The Quantum Insider
Market Map

(https://thequantuminsider.com/data)

DARIO GIL (HTTPS://THEQUANTUMINSIDER.COM/TAG/DARIO-GIL/), GLOBAL (HTTPS://THEQUANTUMINSIDER.COM/TAG/GLOBAL/), GLOBAL LEADER (HTTPS://THEQUANTUMINSIDER.COM/TAG/GLOBAL-LEADER/), IBM (HTTPS://THEQUANTUMINSIDER.COM/TAG/IBM/), IBM RESEARCH (HTTPS://THEQUANTUMINSIDER.COM/TAG/IBM-RESEARCH/), INTELLECTUAL PROPERTY (HTTPS://THEQUANTUMINSIDER.COM/TAG/INTELLECTUAL-PROPERTY/), PATENT APPLICATIONS (HTTPS://THEQUANTUMINSIDER.COM/TAG/PATENT-APPLICATIONS/), PATENTS (HTTPS://THEQUANTUMINSIDER.COM/TAG/PATENTS/), US (HTTPS://THEQUANTUMINSIDER.COM/TAG/US/)

Nev
Quantum Comp
Natic
Resec
Capital N
Exclus
Insig
Educa
Interv
Mec
Repc
Abou
Intellig
Marke
Jok
CONTACT US(HTTPS://WWW.THEQUAI
SUBSC
METAVERSE INSIDER(HTTPS://
GUEST
(HTTPS://WWW.THEQUANTUMIN

Nev
Quantum Comp
Natic
Resea
Capital N
Exclus
Insig
Educa
Interv
Mec
Repc
Abou
Intellig
Marke
Jol
CONTACT US(HTTPS://WWW.THEQUAI
SUBSC
METAVERSE INSIDER(HTTPS://
GUEST
(HTTPS://WWW.THEQUANTUMIN

(https://thequantuminsider.com/author/matt-swayne/)

MATT SWAYNE
(https://thequantuminsider.com/author/matt-swayne/)
Matt Swayne is a contributor at The Quantum Insider. He focuses on breaking news about quantum discoveries and quantum computing.

SHARE THIS ARTICLE

Leave a Reply

You must be logged in (https://thequantuminsider.com/tqiadmin?redirect_to=https%3A%2F%2Fthequantuminsider.com%2F2021%2F01%2F12%2Fibm-research-reports-receiving-more-than-9130-patents-in-2020-quantum-computing-getting-ever-better%2F) to post a comment.

RELATED ARTICLES

(https://thequantuminsider.com/2022/09/27/quantum-matters-a-geopolitical-challenge-of-quantum-proportions/) **Quantum Matters: A Geopolitical Challenge of Quantum Proportions (https://thequantuminsider.com/2022/09/27/quantum-matters-a-geopolitical-challenge-of-quantum-proportions/)** SEPTEMBER 27, 2022

(https://thequantuminsider.com/2022/09/27/aquarian-space-american-binary-team-up-to-bring-telecom-carrier-grade-post-quantum-encrypted-internet-to-solar-system/) **Aquarian Space & American Binary Team Up to Bring Telecom Carrier Grade Post-Quantum Encrypted Internet to Solar System (https://thequantuminsider.com/2022/09/27/aquarian-space-american-binary-team-up-to-bring-telecom-carrier-grade-post-quantum-encrypted-internet-to-solar-system/)** SEPTEMBER 27, 2022

(https://thequantuminsider.com/2022/09/26/caltech-led-research-team-finds-traditional-computers-can-solve-some-quantum-problems/) **Caltech-led Research Team Finds Traditional Computers Can Solve Some Quantum Problems (https://thequantuminsider.com/2022/09/26/caltech-led-research-team-finds-traditional-computers-can-solve-some-quantum-problems/)** SEPTEMBER 26, 2022

The Quantum Insider is the leading provider of media and market intelligence on the quantum technology industry.

Email

You can unsubscribe anytime. For more details, review our Privacy Policy.

SUBSCRIBE

(https://www.linkedin.com/company/the-quantum-daily/) (https://twitter.com/QuantumDaily) (https://www.youtube.com/channel/UClbf-5iPFjQ-Y3RyfQ9/featured) (https://www.instagram.com/thequantuminsider) (https://www.facebook.com/The-Quantum-Insider-105937977453873/) (https://www.tiktok.com/@thequantuminsider)

NAVIGATE

Home
Daily
Exclusives
Marketing Solutions
Industry Intelligence
Jobs Board
About Us
Contact Us
Privacy Policy
Terms And Conditions
Editorial Policy

CONTACT US

Email Us(mailto:hello@thequantuminsider.com)

GUEST POST

Learn How(https://www.thequantuminsider.com/press-release/)
Register(https://www.thequantuminsider.com/reg/)
Sign In(https://www.thequantuminsider.com/reg/)

Nev
Quantum Comp
Natic
Resea
Capital M
Exclus
Insig
Educa
Interv
Mec
Repo
Abou
Intellig
Marke
Jok

CONTACT US(HTTPS://WWW.THEQUAI

SUBSC

METAVERSE INSIDER(HTTPS://

GUEST (HTTPS://WWW.THEQUANTUMIN

DESIGNED BY WEB SHARX (HTTPS://WWW.WEBSHARX.CA/)

IBM Tops U.S. Patent List for 28th Consecutive Year with Innovations in Artificial Intelligence, Hybrid Cloud, Quantum Computing and Cyber-Security

More Than Quarter Century of Patent Leadership Demonstrates IBM's Long-Term Commitment to a Culture of Scientific Discovery and Innovation

Jan 12, 2021

ARMONK, N.Y., Jan. 12, 2021 /PRNewswire/ -- IBM (NYSE: IBM) scientists and researchers received 9,130 U.S. patents in 2020, the most of any company, marking 28 consecutive years of IBM patent leadership. IBM led the industry in the number of artificial intelligence (AI), cloud, quantum computing and security-related patents granted.

> "The world needs scientific thinking and action more than ever," Darío Gil, SVP and Director of IBM Research

"The world needs scientific thinking and action more than ever. IBM's sustained commitment to investing in research and development, both in good and in challenging times, has paved the way for new products and new frontiers of information technology that have greatly benefited our clients and society," said Darío Gil, Senior Vice President and Director of IBM Research. "The culture of innovation at IBM is stronger than ever, thanks to our inventors worldwide who devote themselves to advancing the boundaries of knowledge in their respective fields every single day."

IBM led the industry in the number of U.S. patents across key technology fields:

- **Making AI More Intuitive**
  - IBM received more than 2,300 AI patents as inventors developed new AI technologies to help businesses scale their use of AI. Patents in this area ranged from technology to make virtual agents more responsive to emotions when speaking to customers, to AI that can help people make difficult decisions -- summarizing key decision points from a variety of information sources, both written and verbal, and presenting them in easy-to-understand visualizations. IBM is focused on delivering innovations in natural language processing, automation and building trust in AI, and continually infusing new capabilities from IBM Research into our IBM Watson products. In 2020, this included the IBM Watson team announcing the first commercialization of capabilities from Project Debater – a technology that digests massive amounts of text and constructs a well-structured speech on a given topic and delivers it with clarity and purpose.

- **Streamlining Hybrid Cloud Deployments at the Edge**
  - IBM received more than 3,000 patents related to cloud and hybrid cloud technologies. One of the crucial decisions CIOs face today is determining which data will be processed on premises and which will be processed in the cloud. IBM inventors developed a technology to intelligently distribute the data processing components between the cloud, the edge and computing devices in-between. It offers the potential to greatly optimize the hybrid cloud for IoT workloads – such as GPS-generated driving instructions - that are sensitive to latency. Edge and hybrid cloud offerings are crucial parts of IBM's product roadmap. In 2020, they included the launch in May 2020 of the IBM Edge Application Manager, an autonomous management solution to enable AI, analytics and IoT enterprise workloads to be deployed and remotely managed, delivering real-time analysis and insight at scale. In addition, in November 2020, IBM announced the IBM Cloud for Telecommunications to help companies unlock the power of edge and 5G in November 2020. The holistic hybrid cloud offering leverages IBM's innovative encryption capabilities, designed to enable mission-critical workloads to be managed consistently from the network core to the edge, to position telecom providers to extract more value from their data while they drive innovation for their customers.
- **Laying the Foundation for Powerful Quantum Applications**
  - Quantum computing is a major focus for IBM and this is reflected in IBM's leadership in quantum computing patents obtained. One patent, for example, simplifies the mapping of quantum molecular simulation on a quantum computer. As a result, researchers will be able to explore simulating chemical reactions on quantum computers to understand how and when the discovery process around new materials and new pharmaceuticals will be revolutionized. IBM was also granted a patent that sets the foundation for investigating more accurate and efficient risk analysis calculations on a quantum computer. These ideas are already being extended by research done in collaboration with leading financial institutions.
- **Maximizing Security for the World's Most Sensitive Data**
  - As enterprises work to protect their data, particularly in highly-regulated industries, IBM inventors received more than 1,400 security-related patents. One of the patents is used for fully homomorphic encryption (FHE), an IBM-pioneered method of performing computation on data that remains encrypted while being processed in order to maximize security for data in use. Previously, processing encrypted data required decryption before processing and re-encrypting the results, thus making data more vulnerable while unencrypted. IBM inventors patented a technique that allows encrypted data to be organized so that FHE vector comparison operations can be performed efficiently and maximizes the security of the data. IBM Security launched a service that allows companies to experiment with fully homomorphic encryption in December of 2020.

Patents were awarded to more than 9,000 inventors located in 46 U.S. states and 54 countries. Since 1920, IBM has received more than 150,000 U.S. patents and played a crucial role in innovations ranging from magnetic storage to laser eye surgery. IBM's culture of scientific research is integral to the company's legacy of innovation that matters to our clients and to the world. To that end, in April 2020, IBM announced that it was a founding partner of the Open COVID Pledge, which grants free access to the patents and patent applications of its portfolio of more than 80,000 patents worldwide to those developing technologies to help diagnose, prevent, contain or treat coronaviruses.

Read more about IBM's patent leadership here.

*2020 patent data is sourced from IFI Claims Patent Service: http://www.ificlaims.com.

Hugh Collins
IBM Research Communications
hughdcollins@ibm.com

SOURCE IBM Research

Subscribe to email

Subscribe to email

Release Categories

AI

Quantum/Innovation

More Articles

Saudi Data, AI Authority (SDAIA) and Ministry of Energy Partner with IBM to Accelerate Sustainability Initiatives in Saudi Arabia Using AI

IBM Acquires Dialexa to Speed Digital Innovation

IBM Study: Supply Chain Leaders Are Investing in AI and Automation to Navigate Supply Chain Uncertainties and Improve Sustainability

Subscribe to email

Additional Assets

Key Dates from US Comprehensive State Privacy Laws

iapp

LEGEND

CALIFORNIA
CCPA – California Consumer Privacy Act
CPRA – California Privacy Rights Act
CPRA – CPRA Ballot Initiative
CPPA – California Privacy Protection Agency

VIRGINIA
Virginia's Consumer Data Protection Act

COLORADO
Colorado Privacy Act

CONNECTICUT
Connecticut Personal Data Privacy and Online Monitoring Act

UTAH
Utah Consumer Privacy Act

2020
2021
2022
2023
2024
2025

JAN. 1, 2020
CCPA effective date.

JULY 1, 2020
CCPA enforcement date.

JAN. 1, 2022
CPRA look-back period begins (CPRA Ballot Initiative Section 31(a)).

JULY 8, 2022
CPPA begins formal rulemaking process to update existing **CCPA** regulations and adopt new regulations.

JAN. 1, 2023
CPRA, which amends the CCPA, becomes fully operative. No longer a right to cure (CPRA Ballot Initiative Section 31(a)).

Operative **CPRA** employee and business-to-business exemptions expire (CPRA Sections 1798.145(m) and (n)).

JAN. 1, 2023
Virginia Law's effective date.

JULY 1, 2023
CPRA enforcement begins (CCPA Section 1798.185(d)).

JULY 1, 2023
Colorado law's effective date (Section 7).

JULY 1, 2023
Connecticut law's effective date.

DEC. 31, 2023
Utah law's effective date (Section 17).

JULY 1, 2024
Colorado's law requires universal opt-out mechanism (Section 6-1-1306(1)(a)).

JAN. 1, 2025
Connecticut deadline for controllers to allow a consumer to opt out through an opt-out preference signal (Section 6(e)(1)(A)(ii)).

Connecticut right to cure expires (Section 11(b)). Attorney general has discretion to grant cure period (Section 11(c)).

JAN. 1, 2025
Colorado notice of violation and right to cure expires (Section 6-1-1311(1)(d)).

Note: Particular dates and deadlines should always be verified. IAPP disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability, or fitness for a particular purpose. Nothing herein should be construed as legal advice.

Last updated September 2022.

iapp.org

Licensing / Basics

Licensing

Overview

Licensing choices

Terms and Conditions

Software Subscription & Support (“S&S”)

Overview

Most IBM software is licensed on a trust basis. While there are licensing terms attached to the use of our software, we generally do not enforce these through automatic means. This affords our clients greater flexibility but requires careful management and prompt action should authorized use limits be reached.

There is a lot to learn to fully understand and manage IBM software. This reflects the broad product offering, changing technological landscape and diverse needs of our clients.

This page discusses the primary choices and options available when licensing IBM software. Red Hat software is not covered by this site and is subject to separate license agreements.

Licensing choices

There are various options for licensing and deploying IBM software tailored to suit each client's needs.

Type of license
The three main ways of licensing IBM software are:

Type	Description
Perpetual license	A non-expiring right to use the software. An annual Software Subscription & Support ("S&S") payment grants you access to product support and updates for each year it is purchased. The first year of S&S is often included with the initial license purchase.
Term license	A license that is valid for a predefined period, after which your right to use the software expires. You may terminate the license term early. S&S is included during the term.
Subscription license	Similar to Term licenses except there is no option for early termination. Subscription licenses were formerly referred to as "Committed Term" licenses.

Type of measurement
Every IBM software product is licensed and measured in accordance with a 'license metric'. Some products offer a choice of multiple metrics with different clients' needs in mind.

Read more about license metrics →

Manner of deployment
Traditionally, IBM software was only deployed in a client's own data centers ("on-premise"). The perpetual or term licenses are suited to on-premise deployments.

With clients increasingly choosing to deploy software on infrastructure owned by third parties ("public cloud"), or a mixture of multiple cloud providers and on-premise solutions ("hybrid cloud"), IBM allows clients to deploy their licensed software on a public cloud and also offers subscriptions to IBM's Cloud Services.

IBM licensing is flexible enough to accommodate these different use cases.

Read the 'Public Cloud' licensing guide on the Guides page →
Explore IBM's Cloud Solutions →

Technology

Technology

IBM's licensing embraces a wide variety of technologies, from physical machines to virtual machines

and containers. In addition, IBM's Certified Containers and Cloud Paks allow you to build your solution once and deploy it anywhere, using one set of licensing rules.

Read the 'Cloud Paks' licensing guide on the Guides page →
Read the 'Sub-Capacity' licensing guide on the Guides page →
Read the 'Container Licensing' licensing guide on the Guides page →

Terms and Conditions

Your relationship with IBM is governed by several agreements which set out what is expected in terms of use of our software. These agreements are supplemented by offering-specific documents which set out the licensing terms in more detail. By installing and/or using IBM software, you agree to these terms.

The licensing terms typically relate to how much of the software you can use, how and when you can use it, and/or who can use it. However, there are many other important terms set out in the agreements on matters such as:

- Use restrictions (for example, territories, purpose of use)
- Transfers and change of ownership
- Term of the agreement
- Pricing
- Verification

One of the most important aspects of IBM licensing is the measurement of the license metric. This measurement counts your deployment and/or use of the product.

Read more about Agreements and Contracts →
Read more about License Information documents →
Learn more about license metrics →

Software Subscription & Support ("S&S")

S&S is the term IBM uses for access to product support and updates. Term and Subscription licenses include S&S for the entire period of the license. Perpetual licenses typically include S&S for the first year. After that, you have the option to renew S&S annually or let it lapse. S&S automatically renews, so you must notify IBM if you do not wish to renew.

When buying or renewing S&S for an IBM program you must have enough S&S to cover all your use of that program. You are not permitted to have a 'partly-maintained' deployment. The only exception to this is when you have split your entitlement to an IBM program across multiple Passport Advantage site numbers: you can opt to let S&S lapse for all use at any individual site; but the associated deployments of IBM software must be clearly separated and identifiable from those deployments relating to site numbers with active S&S.

If after letting S&S lapse you decide you want to regain access to the benefits of S&S you must purchase a 'reinstatement' which lasts 12 months. After these 12 months regular S&S automatic renewals recommence.

Once S&S has lapsed on your perpetually licensed IBM program you continue to have the right to deploy the last version update released while your S&S was active. You should ensure that you make and keep a copy of the latest version available prior to S&S lapsing as your access to download links will be restricted once S&S has expired.

Read more about S&S →

This site is intended as a general knowledge resource only and will be updated from time to time so far as reasonably possible. Statements in this site however do not form part of the contract under which a client acquires IBM offerings (the terms of such contract being the exclusive terms between IBM and a client).

Intellectual Property in University and Government Contracts

NYIPLA October 2022 Presentation

Speaker Biographies

- Jennifer Mandina is a contract negotiator at the University of Buffalo focused on industry engagement. She has a BA in English, minor in Accounting; a JD with a concentration in Financing Transaction; and an MS in Biomedical Engineering.
- Derek Maughan is Patent Counsel at Pacific Northwest National Laboratory
- Ankur Parekh has been a practicing attorney for over 15 years. He is currently Senior IP Counsel for the Raytheon Missiles & Defense division of Raytheon Technologies Corporation. He previously worked as IP counsel for the Pratt & Whitney division of Raytheon Technologies and for Legrand, a multinational conglomerate focused on electrical infrastructure and building automation. Ankur started his legal career practicing IP litigation and IP counseling at law firms in New York City.

DISCLAIMER:

THE VIEWS AND OPINIONS EXPRESSED BY THE PRESENTERS, AS COGENT, INTELLIGENT AND WITTY AS THEY MAY BE, ARE NOT THE VIEWS OF THEIR CURRENT OR PAST RESPECTIVE EMPLOYERS (INCLUDING THE UNITED STATES GOVERNMENT OR ANY OF ITS AGENCIES, DEPARTMENTS OR PERSONNEL).

NOTHING IN THIS PRESENTATION IS INTENDED TO CONSTITUTE LEGAL ADVICE AND YOU SHOULD CONSULT YOUR OWN ATTORNEYS AND LEGAL COUNSEL FOR INFORMATION RELATED TO YOUR OWN SPECIFIC LEGAL NEEDS AND POSITION. NO REPRESENTATION OR ATTORNEY-CLIENT RELATIONSHIP BETWEEN THE PRESENTERS AND ANYONE IS CREATED BY THIS PRESENTATION OR ANY FOLLOW-ON QUESTIONS OR ANSWERS THAT MAY FOLLOW.

Agenda

- Ownership and rights to IP created by universities and in the performance of government contracts
- Technology Transfer by Universities
- Additional Agreements Used By Universities Containing IP Terms
- Special Issues in Contracting with DOE
- Some Advanced IP Topics in Government Contracting

IP Ownership and Rights Created During University Sponsored Research and During Federally Funded R&D

- Primary forms of IP created: inventions, technical data (proprietary information, trade secrets), and software
- University research can be sponsored by the U.S. Government or a private organization
- When university research is sponsored by a private organization, the IP rights are determined by an agreement
  - Generally, the university will own the IP it creates
  - Generally, the private organization will get a license of a scope determined through negotiation (or selection from a list of options)
- Comparison: R&D by a private corporation can be funded by the U.S. government or at private expense (IR&D)

University SRAs

- SRA = Sponsored Research Agreement
- Sponsored Research Agreements are used whenever our industry partners engage with us for research.
- UB offers three different options from which to begin negotiations. All are designed to answer questions about IP. The three options are:
  - Exclusive option to negotiate license terms to any resultant IP
  - Pre-negotiate terms to any potential resultant IP
  - Exclusive license to any resultant IP
- SRAs:
  - Clarify the work that will be performed and its related deliverables
  - Have a clearly defined budget and milestones
  - Negotiate sponsor’s rights to pre-publication review to identify any sponsor proprietary information and any disclosed inventions for which a pre-publication patent application filing may be warranted.

How Corporations Think About Sponsoring University Research

- Corporations generally like to use universities for basic research / early-stage technology development
- Many universities today offer to later-stage technology development at a lower cost than commercial vendors
- While the lower cost may be attractive to some at the corporation, counsel must advise the corporation on many issues presented by this approach

Issues Presented by Using University for Later Stage Development

- Universities will generally own the IP they create
- Unlike a commercial vendor, a university will generally not agree to any warranties, indemnities, or carveouts to a consequential-damages waiver
- Many universities demand indemnification from the corporation for any liability they experience from the corporation's use of the research results
- Universities are generally unwilling or, in the case of state universities, unable to negotiate choice of law, choice of venue, and ADR options
- Many universities will not work with ITAR technical data
- Universities will often not agree to long protection periods for any company background proprietary information that the company needs to disclose for the development work

DoE Sponsored Research Agreements

- SPP (Strategic Partnership Projects –formerly WFO)
  - Standard-Sponsor pays full cost reimbursement, accepts standard DOE terms or DOE approves of modifications (See DOE order 481.1)
  - ACT- Contractor accepts full responsibility for fulfilling SPP terms to DOE including full cost-reimbursement
    - Contractor and ACT Participant can then negotiate other terms (including IP)
    - Requires additional disclosures and approvals
- CRADA- Cooperative Research and Development Agreement (DOE Order 483.1)
  - Must have collaboration, CRADA partner provides in kind or in-cash support, leverages private and government contributions, standard terms and conditions flow from Order

CRADAs for Universities

- CRADA = Collaborative Research and Development Agreement
- CRADAs are used to whenever two institutions are working together to perform in-kind research
- It is a standard that the institution that is primarily driving the research supplies the CRADA
- CRADAs:
  - Clearly define each investigators contribution
  - Permit joint and sole publications
  - Resolve IP ownership

IP Created in the Performance of U.S. Govt Contracts

- Inventions
  - Federal procurement of R&D – governed by the Bayh-Dole Act
  - Cooperate R&D w/ government – subject to terms of agreement
- Technical / Data Software
  - Federal procurement of R&D – governed by FAR (and DFARS) and SBIR Act
  - Cooperative R&D w/ government – subject to terms of agreement (CRADA)
  - Generally
    - Contractor owns the technical data and software it creates, even when developed at exclusively at government expense
    - USG gets a license to the technical data / software it creates with federal funding or otherwise delivers to USG in performance of the contract; license scope varies

Bayh-Dole Act

- Codified at 35 U.S.C. §§ 200–212; implementing regulations at 37 C.F.R. §§ 401.1–401.17
- Under Bayh-Dole, the Contractor can elect title to the inventions it creates during Federally funded R&D
- U.S. Government gets a broad license to practice and have practiced the invention for government purposes
- Bayh-Dole was a sea change when it was enacted in 1980; prior to Bayh-Dole, U.S. government owned all inventions created during Federally funded R&D and it licensed only a small percentage of them

Bayh-Dole Act – Some Major Requirements

- Contractor must:
  - Report subject inventions to the U.S. Government within 2 months the inventor's submission of a written invention disclosure;
  - elect title to those inventions within 2 years of disclosure to the agency
  - timely file patent application;
  - timely inform USG of intention not to file a patent application or continue prosecution of patent application; and
  - contractually require employees to disclose inventions created during federally funded R&D and to assign those inventions to the employer.
- Any exclusive licensee of the right to use or sell the invention in the United States must agree that articles embodying the invention are substantially manufactured in the United States

35 U.S.C. 203 March-In Rights

- U.S. Government can force the granting of licenses, if:
  - patent owner has not made sufficient efforts to commercialize the invention;
  - action is necessary to alleviate health or safety needs;
  - action is necessary to meet requirements for public use specified by Federal regulations and such requirements are not reasonably satisfied by the contractor, assignee, or licensees; or
  - holder of exclusive right to use or sell any subject invention in the United States has either not agreed to or is in breach of its agreement to require substantial manufacture of articles embodying the invention in the United States.
- **U.S. Government has never invoked march-in rights**

Substantial U.S. Manufacture

- 35 USC 204- Items for sale in the United States must be substantially manufactured in the United States

- New declaration of exceptional circumstance- all items sold that utilize the technology developed under the funding agreement must be substantially manufactured in the United States

Ownership/Rights in Technical Data / Software Created/Delivered During Federally Funded R&D

- Contractor will generally own the technical data/software it creates, and U.S. Government gets a nonexclusive license
- U.S. Government's rights in such technical data / software for Federal Procurement of R&D under FAR 15
  - Scope of rights
    - Unlimited Rights
    - Limited/Restricted Rights
    - Government Purpose Rights (defense contracts only)
    - Specifically Negotiated License Rights
    - Commercial Rights
  - Expense determinations made at lowest practicable level
  - Contractor must assert data rights that are more restrictive than unlimited rights
  - Data/software must be properly marked when delivered to the U.S. Government

Ownership/Rights in Technical Data / Software Created/Delivered During Performance of SBIR Contract

- U.S. Government gets unlimited rights in background IP that contractor delivers to it
  - Contractors should endeavor to deliver form, fit, function data instead of valuable background IP
- U.S. Government gets SBIR data rights in data/software created by contractor during performance of the SBIR contract
  - SBIR data rights is similar to limited/restricted rights data except there is a fixed time period of protection, which is up to 20 years

Ownership/Rights in Technical Data / Software Created/Delivered During Performance of Cooperative R&D

- U.S. Government will not disclose proprietary background IP it receives from private research partner to third parties
- U.S. Government will not disclose new data / software created by the private research partner during the collaboration and potentially certain new data / software that the government's employees create during the collaboration for up to **five** years (longer protection periods can be authorized)

TECHNOLOGY TRANSFER BY UNIVERSITIES

Technology Transfer: What Is It?

- *General Definition: Dissemination of skills, knowledge and technology to another party for some benefit*
- Specific Definition: University Technology Transfer extends the benefit provided through federal funding by moving research closer to commercialization.
- This function is traditionally viewed as the patenting, marketing, and licensing University technologies.

Licenses

- Licenses are used to transfer commercialization rights of university intellectual property to an industry partner
- It is a standard that the organization that owns the technology drafts the license
- Standard license terms include milestones, royalties, liability, and indemnification provisions
- Because many university technologies are early stage, many of them are licensed to start ups and UB has a specific licensing program for faculty start ups.

UB Invention Lifecycle

- New Technology Disclosure (“NTD”)
- Report to sponsor
  - Federal, Institution, Corporation
- Assessments
  - Intellectual Property and Market Opportunity
- Elect title (Federal) and Inventor assignment
- File for patent/copyright
- Marketing/Customer Discovery
- Licensing

Technology Transfer Assessment

Lab to Market

- **Strength of intellectual property protection**
- Novelty, non-obviousness, usefulness, enablement
- Type: Composition, Device, Process
- Enforcement (detection and cost/benefit)
- Design around
- **Commercial opportunity**
- Solves a significant problem in the market
- Defined customer
- Sustainable competitive advantages
- Size and growth of the potential market
- **Stage of development**
- Investment and risk

Risk
Technical
Intellectual Property
Regulatory
Market
Financial

Commercialization: Why will you win?

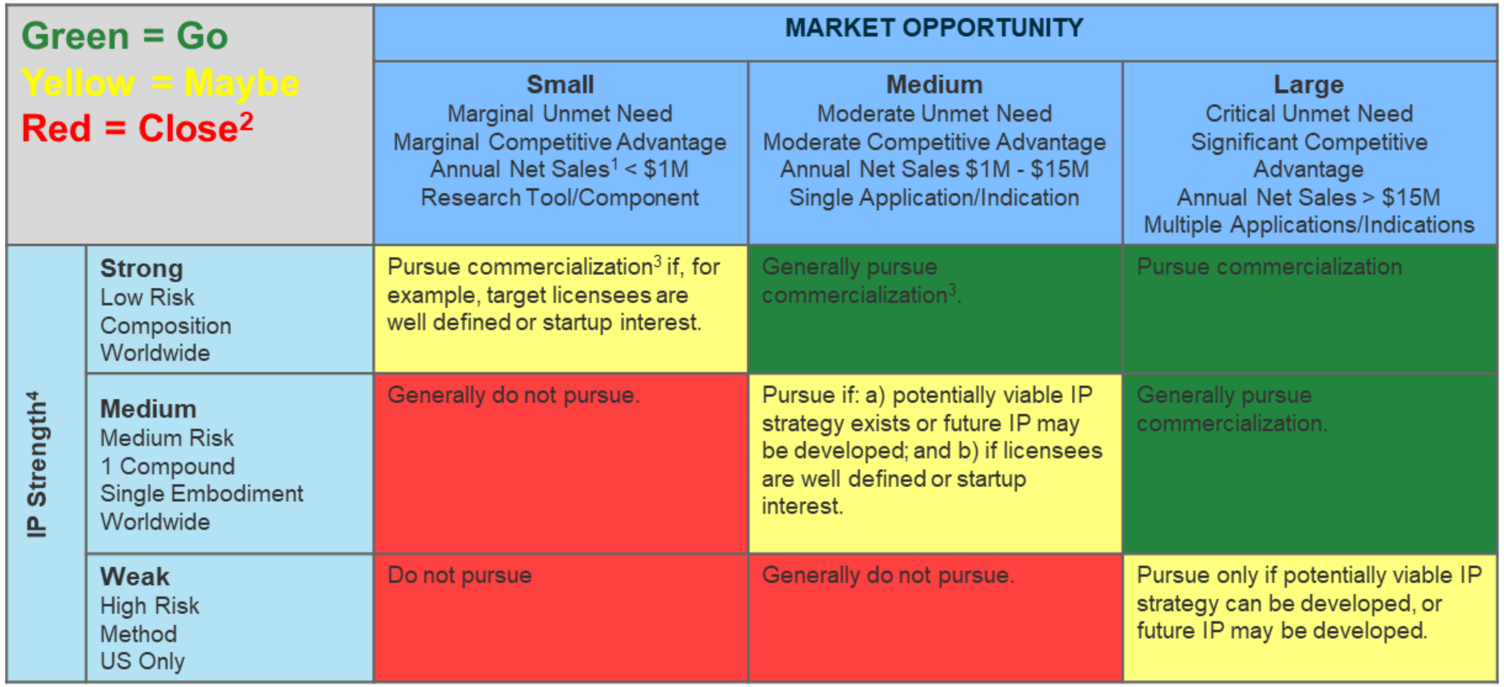
How do target customers rate your features/benefits versus the competition?

Feature/ Benefit	Your Product	Competitor 1	Competitor 2	Competitor 3
Ease of use	+++	+	+	-
Reliability	++	++	+	+
Price	+++	+	++	++
Safety	++	++	+	+
Efficacy	+++	+	+	+

Validate your assumptions with customer discovery.

Market Opportunity Assessment

Filing Decision Matrix



Green = Go
Yellow = Maybe
Red = Close[2]
		MARKET OPPORTUNITY		

		Small Marginal Unmet Need Marginal Competitive Advantage Annual Net Sales[1] < $1M Research Tool/Component	**Medium** Moderate Unmet Need Moderate Competitive Advantage Annual Net Sales $1M - $15M Single Application/Indication	**Large** Critical Unmet Need Significant Competitive Advantage Annual Net Sales > $15M Multiple Applications/Indications
IP Strength[4]	**Strong** Low Risk Composition Worldwide	Pursue commercialization[3] if, for example, target licensees are well defined or startup interest.	Generally pursue commercialization[3].	Pursue commercialization
	Medium Medium Risk 1 Compound Single Embodiment Worldwide	Generally do not pursue.	Pursue if: a) potentially viable IP strategy exists or future IP may be developed; and b) if licensees are well defined or startup interest.	Generally pursue commercialization.
	Weak High Risk Method US Only	Do not pursue	Generally do not pursue.	Pursue only if potentially viable IP strategy can be developed, or future IP may be developed.

Notes:

1. Assuming 3% royalty: $1M = $30,000; $15M = $450,000; $33M = $1,000,000
2. There will be exceptional cases where circumstances warrant a provisional filing to allow for further development, IP assessment or customer discovery.
3. Where "commercialization" is used, it means protect IP, conduct customer discovery, pursue POC funds, identify licensees or startup opportunities.
4. When assessing IP strength, refer to Patent Prosecution Guidelines and take into consideration potential IP will or can be strengthened by further planned and funded R&D.

OTHER AGREEMENTS THAT ADDRESS IP ISSUES

What an Agreement Does

- Provides clarity on rights and responsibilities and protects the parties
  - Indemnification – Who is responsible if something goes wrong
  - Term – How long is the relationship and obligations in effect
  - Use – For example, how may the information or materials be used
  - Statement of Work (SOW) – Defines and sets limits on the work to be performed and by whom
  - Budget – How much does the work cost, and when will payments be made
  - Reps and Warranties
  - Limitations of Liabilities
- Enables the investigator to focus on their research

MTAs

- MTA = Material Transfer Agreement
- MTAs are used to memorialize the transfer materials between organizations
- It is a standard that the organization providing the material will supply the MTA
- If the material is not properly brought in:
  - Transfer of material not permitted until resolved
  - Creates question of ownership on inventions
  - Liability/Indemnification

CDAs = NDAs = PIAs

- CDA = Confidential Disclosure Agreement
- NDA = Nondisclosure Agreement
- PIA = Proprietary Information Agreement
- CDAs provide the terms under which confidential information may be exchanged
- It is a standard that the organization providing the confidential information will supply the CDA
- If the information is exchanged without an agreement:
  - May be a publication for patenting purposes – may bar patent protection
  - No limitations on use
  - Liability/Indemnification

VSAs

- VSA = Visiting Scientist Agreement
- VSAs are used whenever an investigator visits another institution to perform work (ex - sabbatical)
- It is a standard that the institution that is hosting the investigator supplies the VSA
- VSAs:
  - Permit research to be openly conducted
  - Contribute to collaboration
  - Resolve IP ownership

IIAs

- IIA = Inter-Institutional Agreement
- IIAS are used whenever investigators from more than one entity contribute to an invention.
- It is a standard that the institution that will be responsible for leading the licensing efforts supplies the IIA.
- IIAs:
  - Define the roles of each institution
  - Determine control of patent process
  - Determine financial contribution to patent costs
  - Determine royalty split
  - List required terms of any license

TAs/SAs

- TA = Testing Agreement
- SA = Services Agreement
- TAs and SAs are used when an organization is using university equipment/employees to conduct standard testing or services.
- Industry prefers to start from their template, all other organizations defer to the service/testing provider.
- TAs and SAs:
    - Specify the work to be performed, as dictated by the entity ordering the test/service
    - Give ownership of the results to the contracting party
    - Are generally silent on IP

CTAs

- CTA = Clinical Trial Agreement
- Clinical Trial Agreements are a type of agreement used to enable human subjects research (ex – Investigational New Drug (IND) study)
- To enable faster execution, there are currently over 20 active Master CTAs used by pharmaceutical companies working with UB
- CTAs:
  - Clarify the work that will be performed ("Protocol")
  - Determine number of study participants/questions about publication/ownership of data and samples
  - Have a clearly defined budget and milestones

SPECIAL ISSUES WHEN CONTRACTING WITH DOE

Office of Science Laboratories

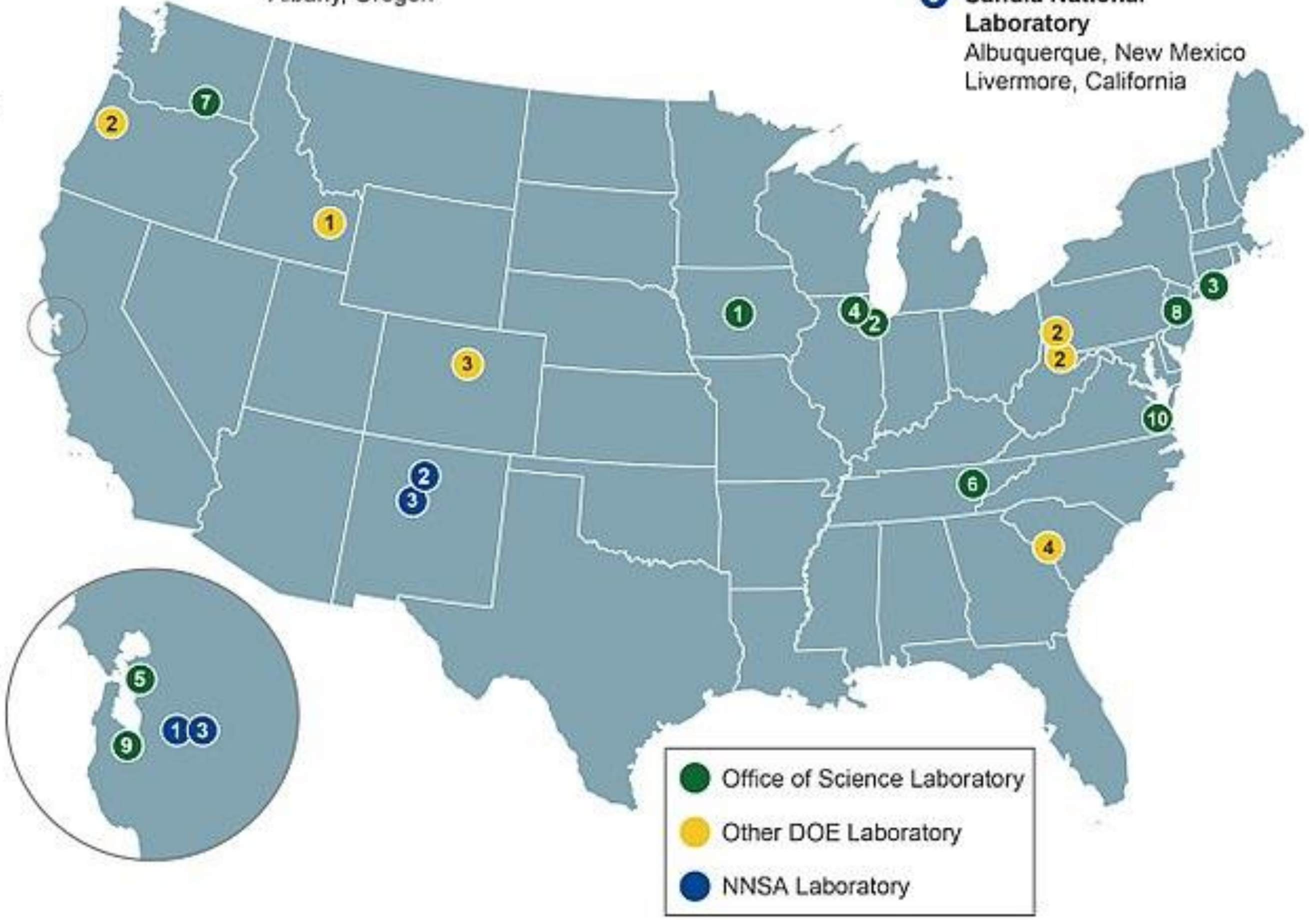
1. **Ames Laboratory**
   Ames, Iowa
2. **Argonne National Laboratory**
   Argonne, Illinois
3. **Brookhaven National Laboratory**
   Upton, New York
4. **Fermi National Accelerator Laboratory**
   Batavia, Illinois
5. **Lawrence Berkeley National Laboratory**
   Berkeley, California
6. **Oak Ridge National Laboratory**
   Oak Ridge, Tennessee
7. **Pacific Northwest National Laboratory**
   Richland, Washington
8. **Princeton Plasma Physics Laboratory**
   Princeton, New Jersey
9. **SLAC National Accelerator Laboratory**
   Menlo Park, California
10. **Thomas Jefferson National Accelerator Facility**
    Newport News, Virginia

Other DOE Laboratories

1. **Idaho National Laboratory**
   Idaho Falls, Idaho
2. **National Energy Technology Laboratory**
   Morgantown, West Virginia
   Pittsburgh, Pennsylvania
   Albany, Oregon
3. **National Renewable Energy Laboratory**
   Golden, Colorado
4. **Savannah River National Laboratory**
   Aiken, South Carolina

NNSA Laboratories

1. **Lawrence Livermore National Laboratory**
   Livermore, California
2. **Los Alamos National Laboratory**
   Los Alamos, New Mexico
3. **Sandia National Laboratory**
   Albuquerque, New Mexico
   Livermore, California



Background

Under Atomic Energy Act (1946, 1954) that established the labs all work and all results of work are to be DOE's and made available to the public. Rights can be waived to certain classes of people under documents called class waivers.

- Economy Act of 1932 provides authorization to do work for other Federal Agencies at DOE facilities
- DOE O 481.1 provides authorization to perform non-federal work for others (SPP)
- DOE O 483.1 provides an authorization to perform CRADAs (Stevenson-Wydler legislation made TT a mission of the laboratories
- IP is dispositioned by virtue of a class waiver wherein DOE waives its automatic full ownership of IP according to certain conditions in applicable circumstances to certain classes of people. The terms of these class waivers are laid out in the class waivers and their associated appendices (A, B, C)

What is a Foreign Sponsor? DOE Order 485.1

“Foreign entities include:

- Any foreign government or foreign government agency, or instrumentality thereof;
- Any international organization
- Any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its territories
- Any form of business enterprise organized or incorporated under the laws of the United States or a State or other another jurisdiction within the United States which is *owned, controlled or influenced by a foreign government agency, firm or corporation* and
- any person who is not a citizen or national of the United States.

Obtaining and Perfecting Rights in IP

- Follow instructions in agreement – recognize that terms typically flow from statute, regulation or administrative document such as a class waiver, know the source documents (ask if you need to) and don't try to vary too far or get too creative, look for preapproved alternative language
- FAR 52.227-14- Rights in Data general-tax payers pay, taxpayers have access unless permission to copyright is obtained
- FAR 52.227-15 –Limited Rights Data Representation
- FAR 52.227-11- Small entities have Bayh-Dole rights in inventions
- FAR 52.227-13 Government owns inventions, Large Entities and Foreign do not have Bayh-Dole Rights and must petition for waiver and exception

Federal Acquisition Regulation

- 52.227-1 Authorization and Consent.
- 52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement.
- 52.227-3, 4, 5 Patent Indemnity.
- 52.227-6 Royalty Information.
- 52.227-7 Patents-Notice of Government Licensee.
- 52.227-9 Refund of Royalties.
- 52.227-10 Filing of Patent Applications-Classified Subject Matter.
- 52.227-11 Patent Rights-Ownership by the Contractor.
- 52.227-13 Patent Rights-Ownership by the Government.
- 52.227-14 Rights in Data-General.
- 52.227-15 Representation of Limited Rights Data and Restricted Computer Software.
- 52.227-16 Additional Data Requirements.
- 52.227-17 Rights in Data-Special Works.
- 52.227-18 Rights in Data-Existing Works.
- 52.227-19 Commercial Computer Software License.
- 52.227-20 Rights in Data-SBIR Program.

Takeaways

- Government terms are often generated through the Administrative Rule Making process and there are limited availabilities to modify.
- 1) Read the standard and compare standard with proposed terms, be willing to agree to the standard or preapproved alternatives.
- 2) Ask for flow downs by citation without amendment
- 3) Points of preference or grammar may need to be set aside
- 4) Understand that terms are written with the taxpayer in mind not the person wanting to do business with the government
- 5) Reasonableness is a different term in the beltway than it is in the rest of the country
- 6) Foreign interest and control is always a concern and a flag.
- 7) Since the terms of the agreement have limited flexibility attorneys can show value by getting in on the front end and structuring the arrangement with the technical folks so that the clients aims are addressed in various ways.
- Look at SOW and funding sources for various elements in a project, where are government use rights and requirements tolerable and not tolerable, look out ahead of time at RFP, are there elements that can be sourced from private resources and use government R&D assets for earlier TRL investments?
- Government use rights does not mean that Government owns or that a pathway is closed it just means that alternative pivots and different planning may be required.

SOME ADVANCED IP TOPICS IN GOVERNMENT CONTRACTING

Authorization & Consent (28 U.S.C. § 1498)

- Most government procurement contracts under FAR 15 have an A&C clause
  - Not always included in other government contracts, such as OTAs, CRADAs, SBIR agreements, etc.
- Under A&C, a contractor can infringe a U.S. patent in its performance of a government contract without liability to the patent owner
  - Limited exception in production contracts for manufacturing procedures or equipment not required to perform the contract
- Patent owner can sue the U.S. Government for the infringement, but the only remedy is reasonable monetary compensation
  - Injunctive relief is not available
  - Suit must be brought in the Court of Federal Claims
- A&C is an application of eminent domain and sovereign immunity
  - Government is "taking" a sublicenseable license under the patent for just compensation and limiting where it can be sued
- A&C does not apply to foreign patents
  - Suit against a foreign subcontractor for infringement of a foreign patent still available
  - Most developed nations have their own version of A&C

Government Contracting vs. Private Contracting

- Private contracting – two parties exercising their freedom to contract to reach any deal they can agree to
- Government contracting – a private contractor negotiating with a government contracting officer who is constrained by laws and regulations as to the scope of the deal
- Private contracting – the deal is governed by the "four corners" of the contract; extrinsic evidence is not admissible unless the contract language is ambiguous
- Government contracting – language that does not appear in the contract can be read into it as a matter of law
  - *Christian* doctrine - *G.L. Christian & Assocs. v. United States*, 312 F.2d 418 (Ct. Cl. 1963)
  - Contract clauses that express a "deeply ingrained strand of public procurement policy" are incorporated by operation of law
  - Government contracts have more than four corners!
  - Does it apply to Bayh-Dole and data-rights framework in FAR/DFARS?

Questions?