Unlock Key Steps to Your Cybersecurity Readiness

Rehmann

EMPOWER YOUR PURPOSE

Meet Our Speakers

Jim Carpp

Chief Digital Officer

james.carpp@rehmann.com

Jim Bruxvoort

Chief Services Officer – Rehmann Technology Services

jim.bruxvoort@rehmann.com

75% of US businesses have associates working remotely

That is a **250%** increase since March

Source: Electric.ai Survey

Home offices and other remote-working setups will redefine supply chain attacks.

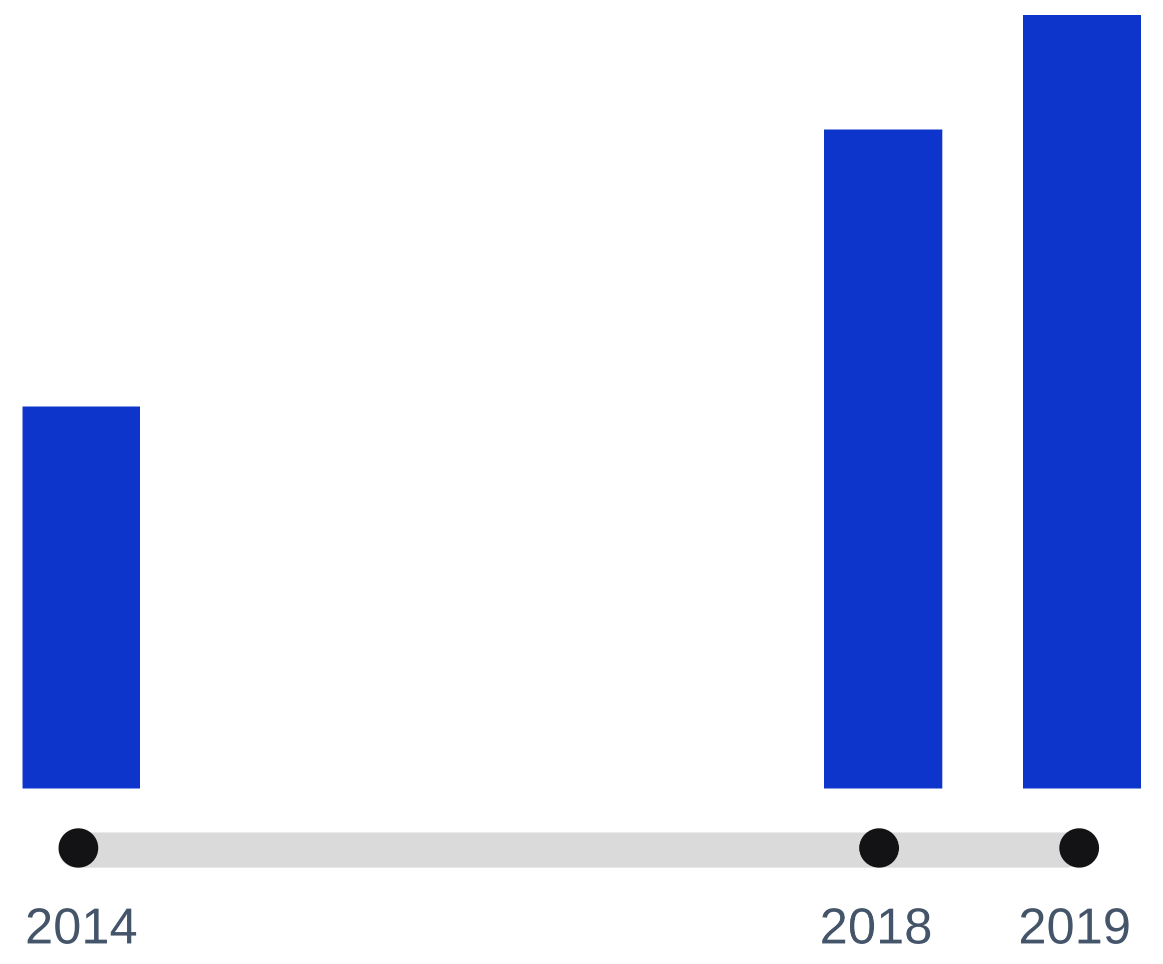
Organizations will have to be wary of risks introduced by work-from-home arrangements and internet-connected home devices that blur the lines in enterprise security.

Source: The New Norm: Trend Micro Security Predictions for 2020

29.6% Chance of a Breach in the Next Two Years

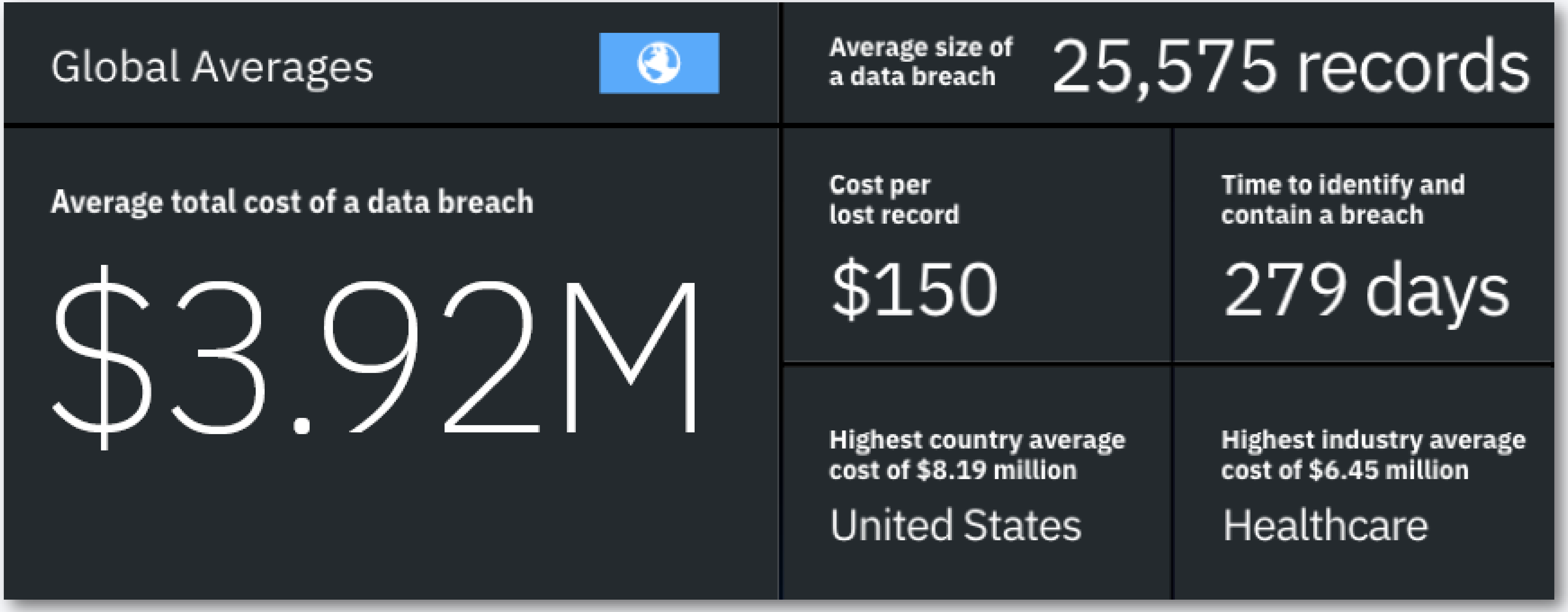
The odds of experiencing a data breach increased

The percentage chance of experiencing a data breach within two years was 29.6 percent in 2019, an increase from 27.9 percent in 2018. In 2014, organizations had a 22.6 percent chance of experiencing a breach within two years.



Source: IBM Security – Cost of a Data Breach Report 2019

Ponemon 2019 - Cost of Breach



Global Averages

Average size of a data breach 25,575 records

Average total cost of a data breach

$3.92M

Cost per lost record

$150

Time to identify and contain a breach

279 days

Highest country average cost of $8.19 million

United States

Highest industry average cost of $6.45 million

Healthcare

Source: IBM Security – Cost of a Data Breach Report 2019

Key findings:

The average total cost of a data breach in the U.S. for the companies studied has grown from $3.54 million in 2006 to $8.19 million in 2019, a 130 percent increase over 14 years.

$\$3.54^{M}$

US total cost in 2006

$\$8.19^{M}$

US total cost in 2019

Source: IBM Security – Cost of a Data Breach Report 2019

Key findings:

The lifecycle of a data breach in the 2019 study was 279 days, 4.9 percent longer than the 2018 lifecycle of 266 days

279 days

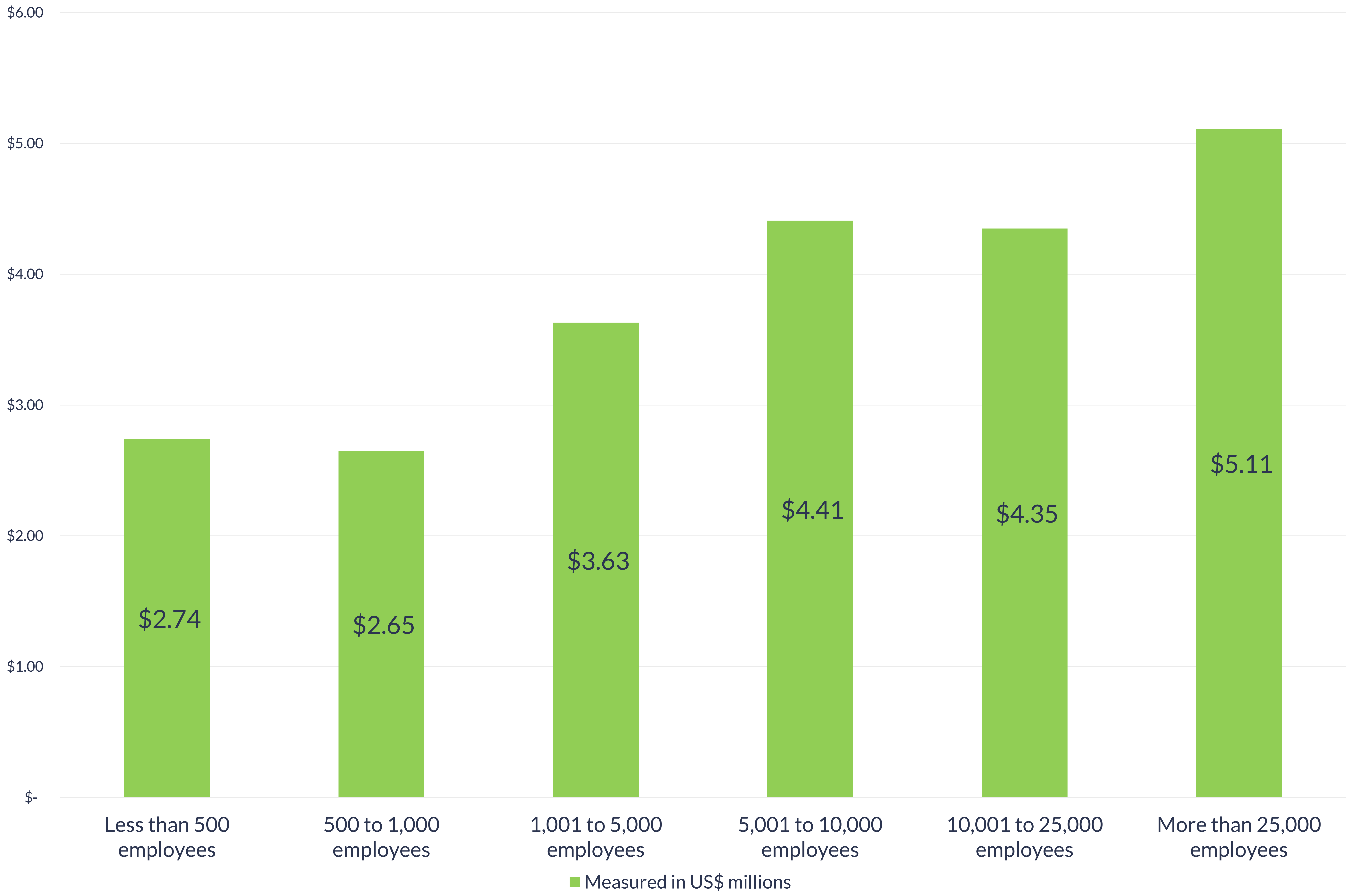
Lifecycle of a data breach in 2019

4.9%

2019 lifecycle is 4.9 percent longer than the 2018 lifecycle of 266 days

Source: IBM Security – Cost of a Data Breach Report 2019

Total Cost of a Data Breach by Organizational Size



Source: IBM Security – Cost of a Data Breach Report 2019

One incident response per month

Average cost: $80,000

Small businesses face disproportionately larger costs relative to larger organizations.

We found significant variation in total data breach costs by organizational size. The total cost for the largest organizations (more than 25,000 employees) averaged $5.11 million, which is $204 per employee. Smaller organizations with between 500 and 1,000 employees had an average cost of $2.65 million, or $3,533 per employee.

Source: IBM Security – Cost of a Data Breach Report 2019

Breach Cost:

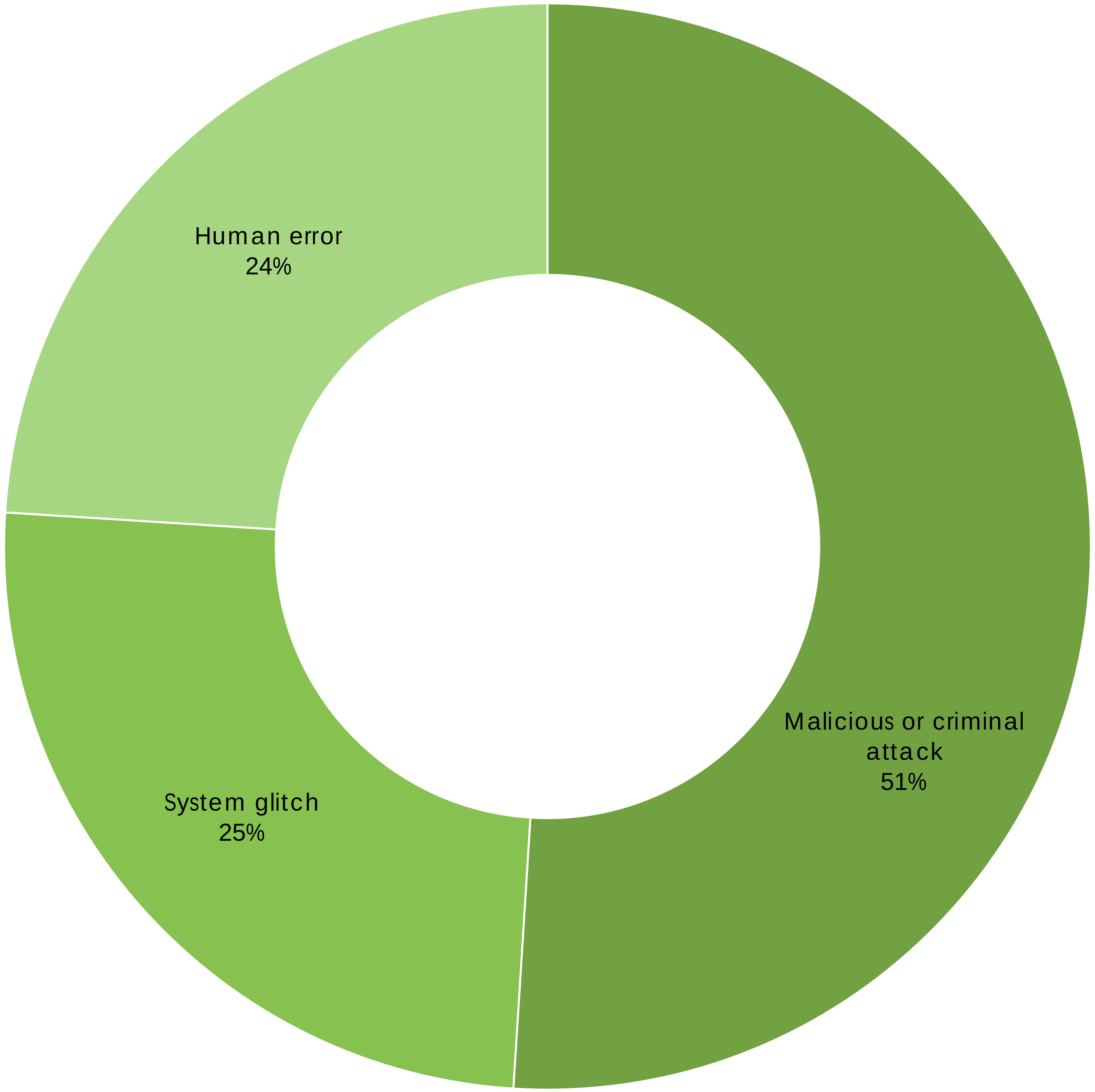
What is Your Exposure?

What is the cost of a breach?

Objective:

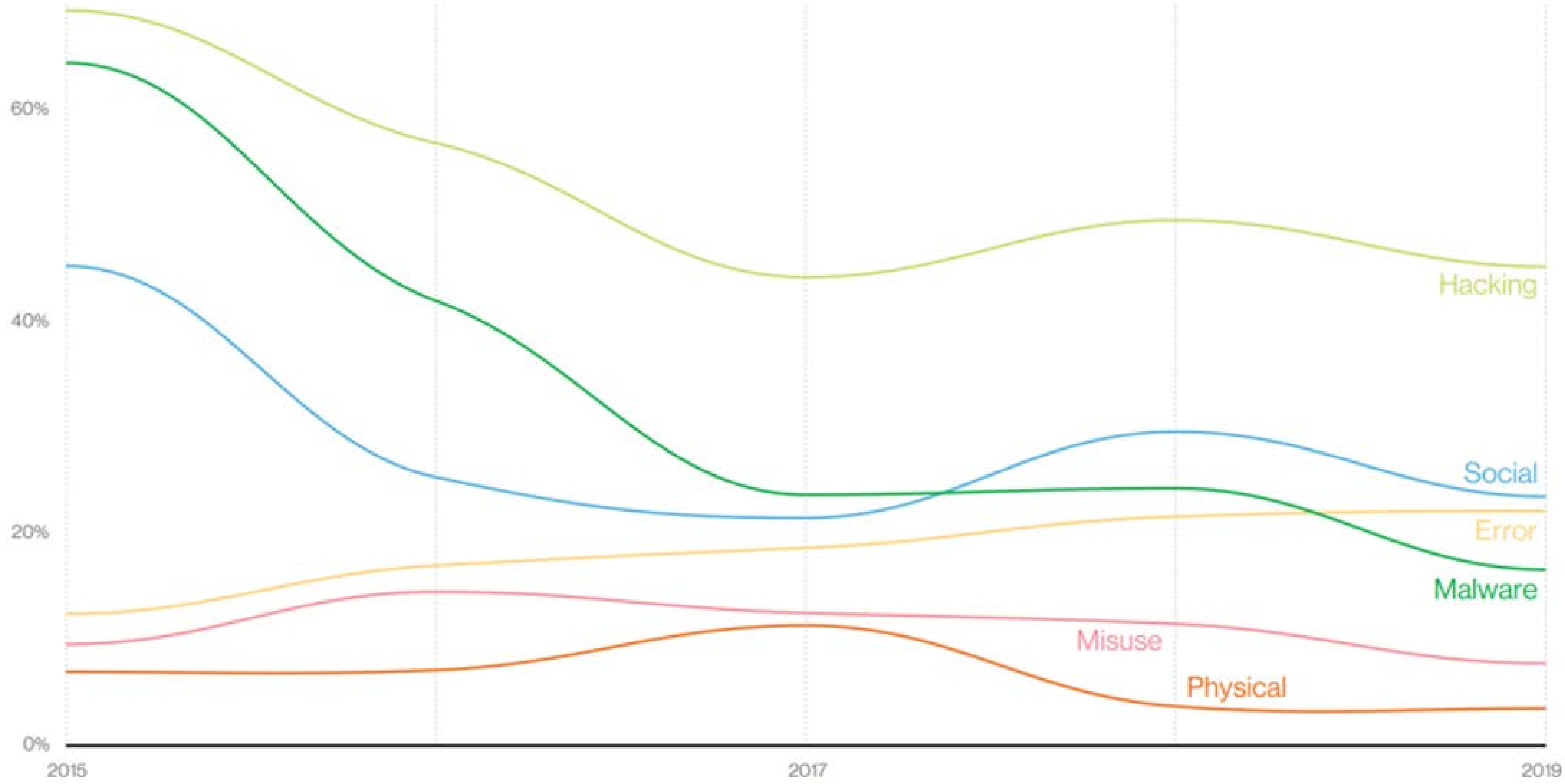
Determine a potential financial impact to your organization in the event of a breach

Data Breach Root Causes



Source: IBM Security – Cost of a Data Breach Report 2019

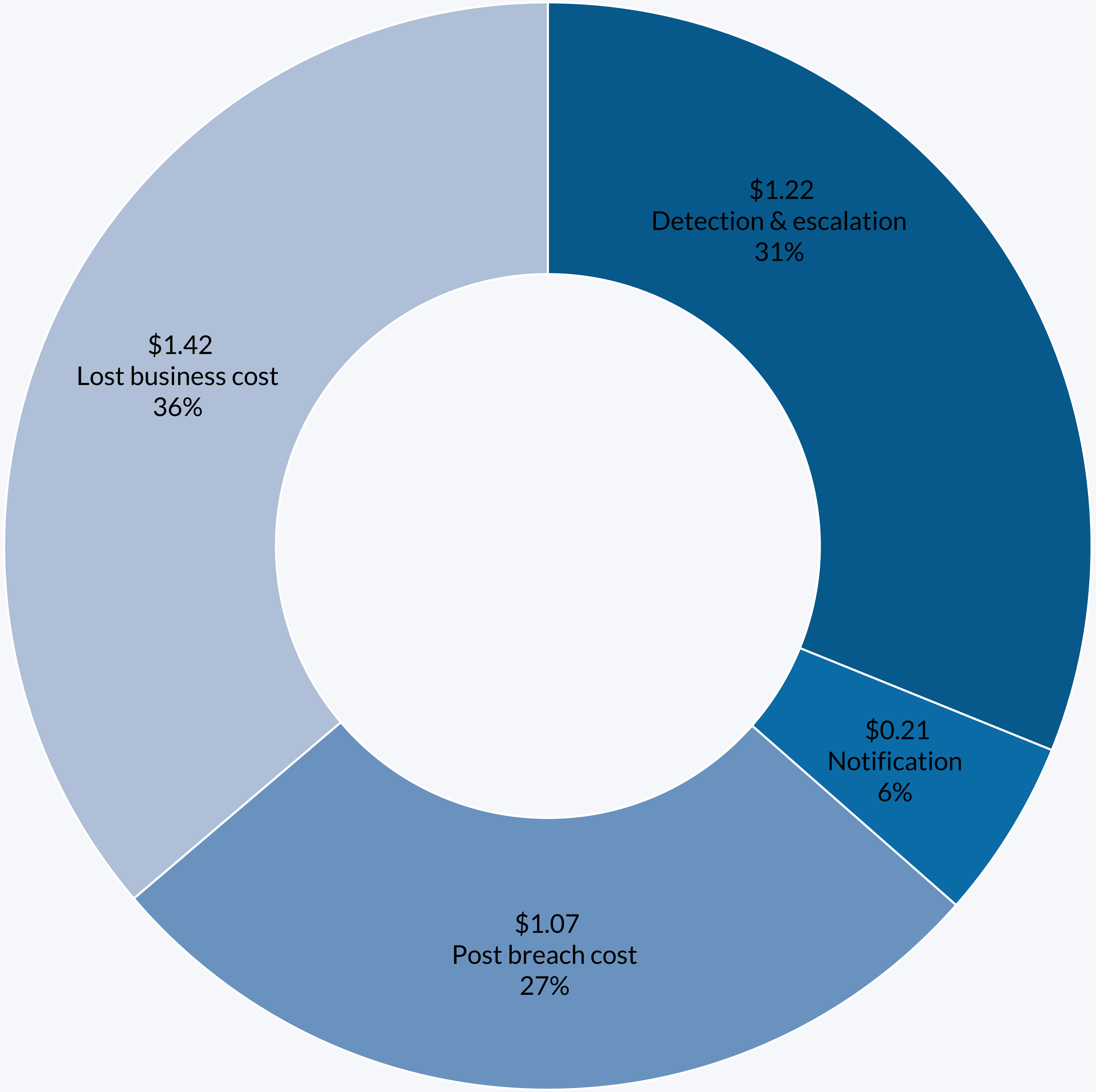
What Are the Actions Over Time?



2020 Data Breach Investigations Report

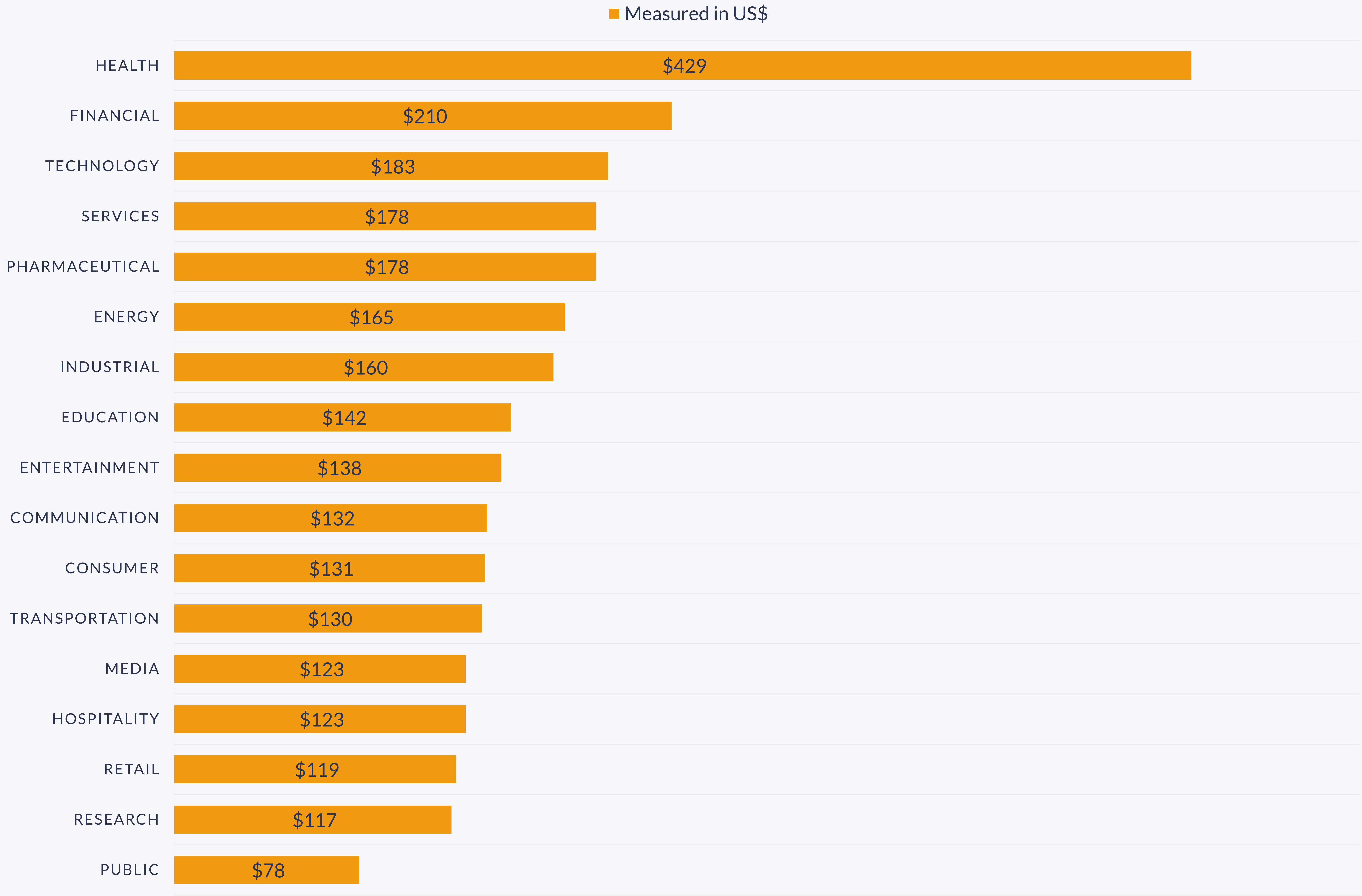
Data Breach Total Cost Broken Down Into Four Cost Categories

Measured in US$ millions



Source: IBM Security – Cost of a Data Breach Report 2019

Average Cost Per Record by Industry Sector



Source: IBM Security – Cost of a Data Breach Report 2019

Potential Exposure – SWAG Calculation

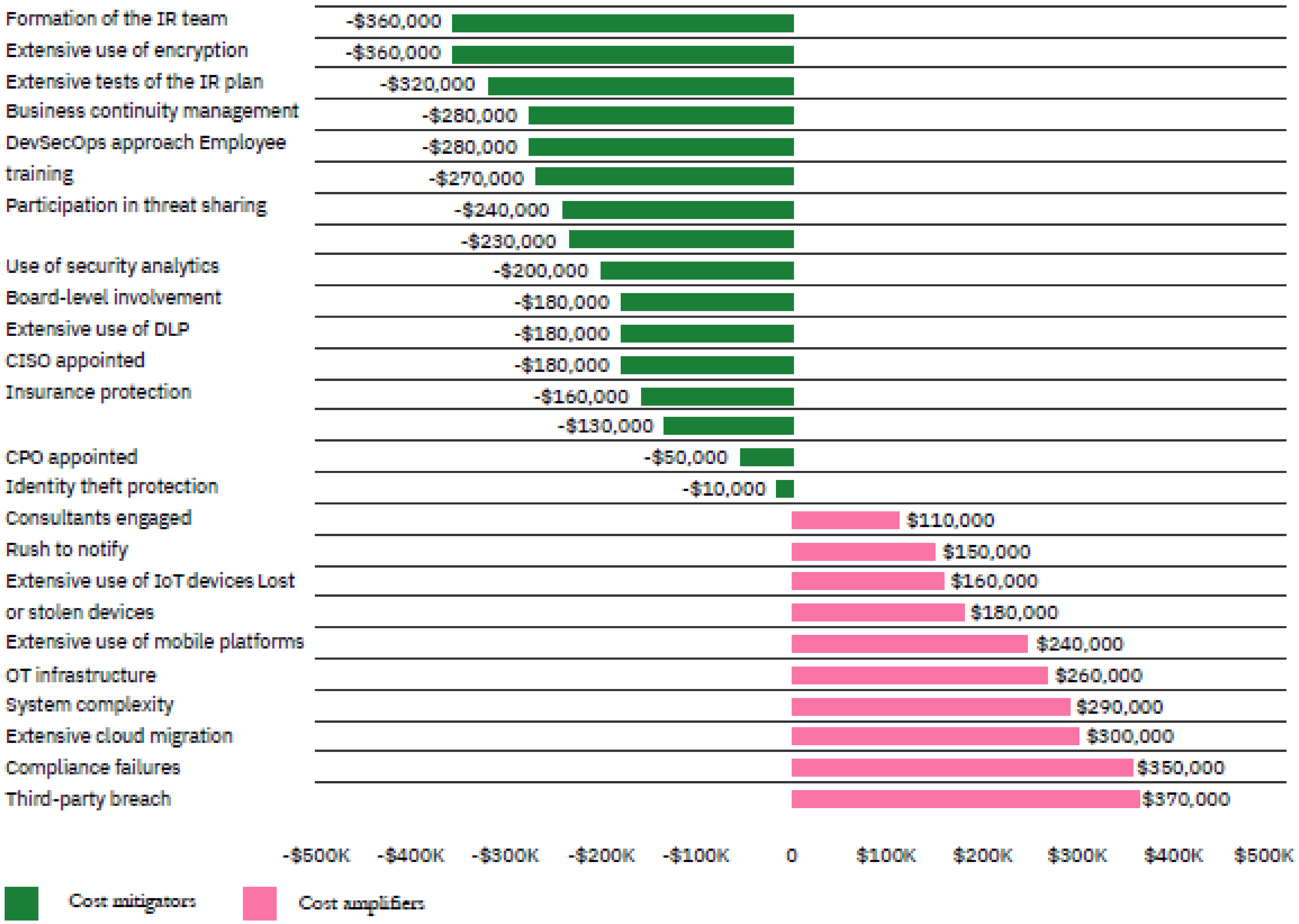
The potential exposure simple calculations:

Number of Records with PII X Cost per record by industry = Exposure

Personally Identifiable Information (PII)

How Factors Increased or Decreased the Total Cost of a Data Breach

Difference from average total cost of US $3.92 million



Source: IBM Security – Cost of a Data Breach Report 2019

The question is – How do your protect yourself?

You can build a comprehensive Cybersecurity Program

What is the state of our security program?

Objective:

Answer a short series of questions to ascertain the current state of the Governance of the Cybersecurity Program

Asset inventory:

Is there an inventory in place with all of the hardware including PCs, server, router, mobile phones?

Critical data:

Has the organization’s critical data been identified?

Data backup:

Is a plan in place for safeguarding your critical data and tested regularly?

What is the state of our security program?

Cyber Security Program:

Has a Cyber Security program been developed, deployed and communicated?

Cybersecurity Program

A solid Cybersecurity Program will encompass:

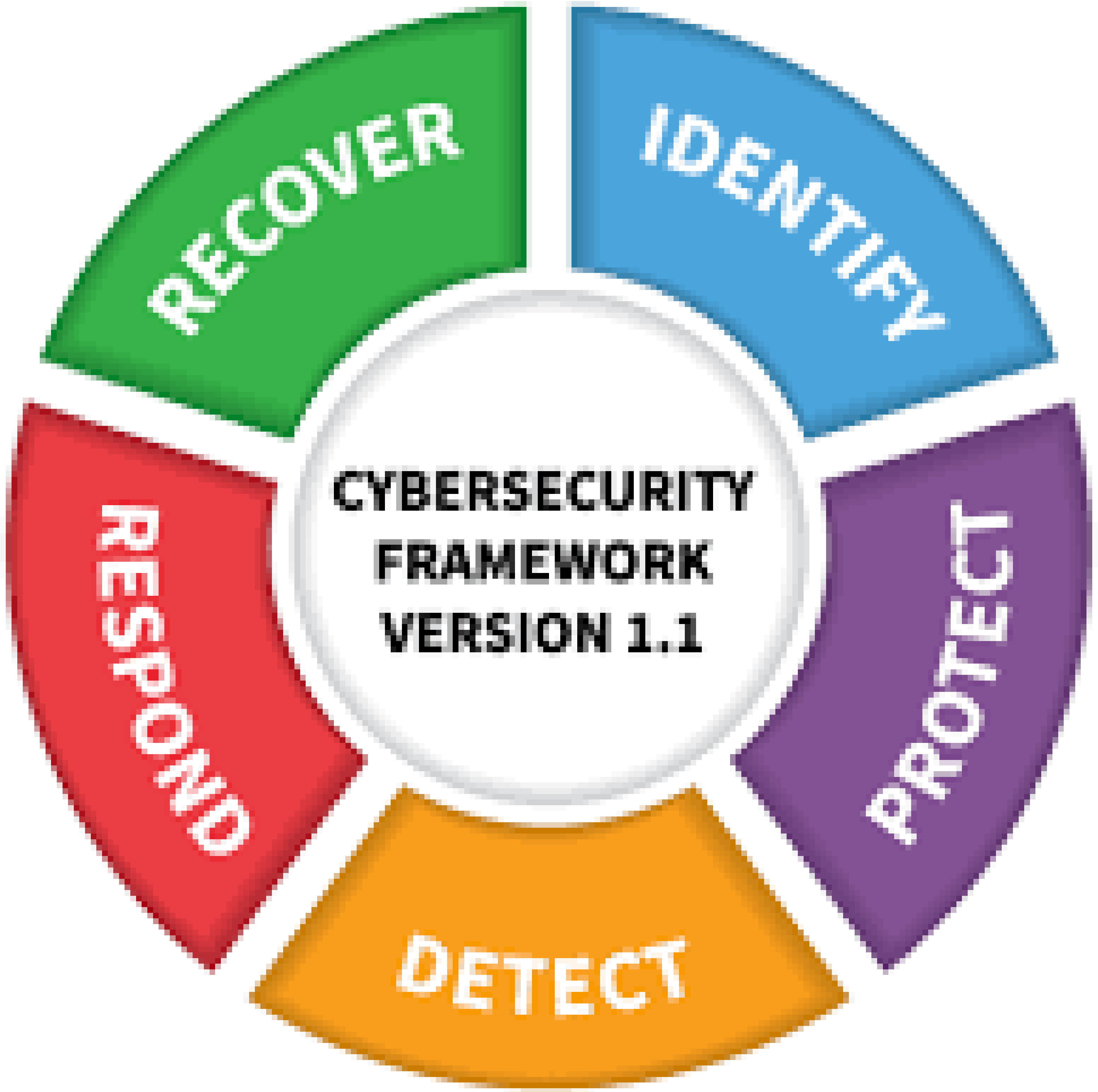
- Governance Strategy
- Leadership – CISO, Steering Committee and Security Team
- Data Management and Protection Strategy
- Risk Assessment – Impact, Likelihood and Priority
- IT Security Policy
- Backup Strategy
- Incident Response Plan
- Business Continuity Plan/Disaster Recovery Plan
- Vendor Management Process

Leverage these standards to build your program

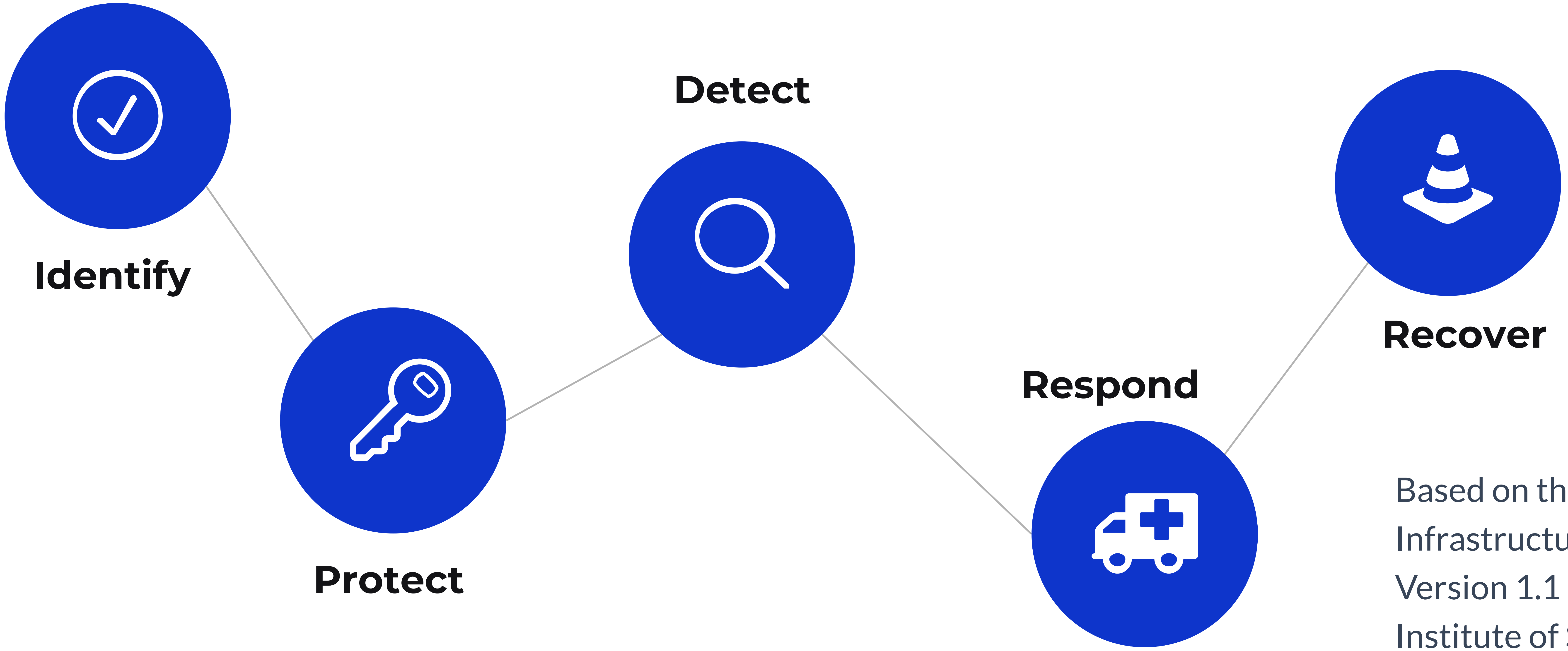
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

1. Critical Infrastructure Cybersecurity - Version 1.1 from the National Institute of Standards and Technology dated April 16, 2018
2. NISTIR 7621 - Revision 1 - Small Business Information Security - The Fundamentals
3. NIST 800 53 Rev 4 and NIST 800 171

NIST – Cyber Security Framework (CSF)



Cyber Security Framework (CSF)



Based on the Critical Infrastructure Cybersecurity - Version 1.1 from the National Institute of Standards and Technology dated April 16, 2018

Word of Caution

There are over 1,500 controls to consider

Difficult to know where to start or…

It is easy to get lost in the details

CSF Framework is Complex

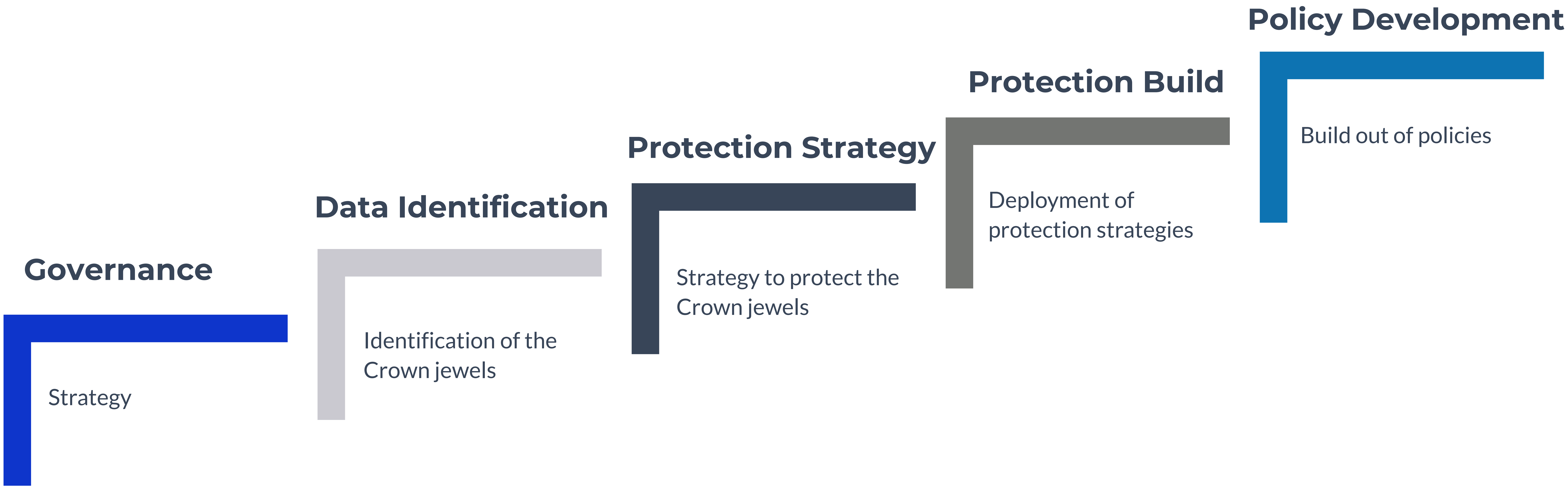
Function	Category	Subcategory	Question:	Answer	Worksho	Priority	RTS Suggestion:	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	Are Physical devices and systems within the organization inventoried?	y/n/na	PDRR	1	Consider leveraging software (passive and active) to document physical devices (e.g., hardware, software, data, and systems hosted externally)	- CIS CSC 1 - https://www.cisecurity.org/controls/inventory-and-control-of-hardware-assets/ - NIST SP 800-53 Rev. 4 CM-8, PM-5 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.AM-2: Software platforms and applications within the organization are	Are software platforms and applications within the organization inventoried?		PDRR	1	Consider leveraging software (passive and active) to document physical devices (e.g., hardware, software, data, and systems hosted externally)	- CIS CSC 2 - https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/ - NIST SP 800-53 Rev. 4 CM-8, PM-5 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.AM-3: Organizational communication and data flows are mapped	Are organizational communication and data flows mapped?		PDRR	3	Ensure that data flow diagrams are in place and document information flow to external parties as well as a validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.	- CIS CSC 12 - https://www.cisecurity.org/controls/boundary-defense/ - NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.AM-4: External information systems are catalogued	Are external information systems catalogued?		PDRR	**3**	Consider cataloguing external information systems at a minimum to include a list of third-party service providers as well as a network diagram is in place and identifies all external connections.	- CIS CSC 12 - https://www.cisecurity.org/controls/boundary-defense/ - NIST SP 800-53 Rev. 4 AC-20, SA-9 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Are resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value?		I	1	Consider prioritizing resources based on their classification, criticality, and business value Institution assets (e.g., hardware, systems, data, and applications) and ensure they are prioritized for protection based on the data classification and business value.	- CIS CSC 13 - https://www.cisecurity.org/controls/data-protection/ - CIS CSC 14 - https://www.cisecurity.org/controls/controlled-access-based-on-the-need-to-know/ - NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Are cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) established?		G	1	Consider documenting the cyber security roles and responsibilities for the entire workforce and third-party stakeholders in the cyber security policy as well as management should hold all parties accountable for compliance.	- CIS CSC 17 - https://www.cisecurity.org/controls/implement-a-security-awareness-and-training-program/ - CIS CSC 19 - https://www.cisecurity.org/controls/incident-response-and-management/ - NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11 - https://nvd.nist.gov/800-53/Rev4/impact/high - https://www.betterteam.com/information-technology-job-descriptions
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	Is the organization's role in the supply chain identified and communicated?		G	3	Determine and communicate the organization's role in the supply chain, if it is determined that is a component of critical infrastructure.	- NIST SP 800-53 Rev. 4 CP-2, SA-12 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Is the organization's place in critical infrastructure and its industry sector is identified and communicated?		G	3	Determine and communicate the organization's place in the critical infrastructure and the industries sector if it is determined that is a component of critical infrastructure.	- NIST SP 800-53 Rev. 4 PM-8 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Are priorities for organizational mission, objectives, and activities established and communicated?		G	3	Consider establishing and communicating priorities for organizational mission, objectives and activities to include: · a formal cybersecurity program that is based on technology and security industry standards or benchmarks. · The board or an appropriate board committee ensures management's annual cybersecurity self-assessment evaluates the institution's ability to meet its cyber risk management standards. · The cybersecurity strategy is incorporated into, or conceptually fits within, the institution's enterprise-wide risk management strategy.	- NIST SP 800-53 Rev. 4 PM-11, SA-14 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Are dependencies and critical functions for delivery of critical services established?		I	3	Consider establishing dependencies and critical functions for delivery of critical services to include: · The critical business processes that are dependent on external connectivity have been identified. · Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.	- NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	Are resilience requirements to support delivery of critical services established for all operating states (e.g. under duress/attack, during recovery, normal operations)?		Policy	3	Consider establishing resilience requirements to support delivery of critical services for all operating states to include: · A business continuity plan (BCP) is in place to identify alternative processes have been established to continue critical activity within a reasonable time period. · A disaster recovery plan has been developed and maintained to support the BCP. · A formal data backup and recovery plan exists for all critical business lines. · An incident response plan is in place to respond and recover to unforeseen events.	- NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-13, SA-14 - https://nvd.nist.gov/800-53/Rev4/impact/high
		ID.GV-1: Organizational	Is an organizational				Consider establishing, maintaining and communicating and organizational cyber security policy which is	- CIS CSC 19 - https://www.cisecurity.org/controls/incident-response-and-management/

Goal – Eliminate the complexity and make it implementable

Rehmann

Cybersecurity Risk Management Foundation

This is a straightforward process designed to take out the complexity and simplify the implementation



Governance

Strategy

Data Identification

Identification of the Crown jewels

Protection Strategy

Strategy to protect the Crown jewels

Protection Build

Deployment of protection strategies

Policy Development

Build out of policies

Cybersecurity Risk Management Process

Governance

- Strategy
- Leadership
- Oversight

- Objective – Establish a governance strategy
- Target Audience – The executive team
- Process - Facilitated session
- Content –
  - Provide High-Level Training
    - Governance
    - Cyber Security Framework
  - Overview of the process
  - Walk through a series of questions to rough in the Cyber Security Framework
- Deliverable –
  - Create a security continuum strategy
  - Identify the key components of the cyber security program
  - Identify a security lead
  - Determine next steps to build out the governance structure

Cybersecurity Risk Management Process

Data Identification

Identification of the Crown jewels

- Objective – Identify critical data and establish a risk-based protection strategy
- Target Audience – Data owners and IT lead
- Process - Facilitated sessions
- Deliverable:
    - Identification of critical asset
        - Data
        - Hardware
        - Software
    - Development of a risk assessment to include:
        - Asset
        - Likelihood
        - Impact
        - Priority
    - Development of a strategy to protect the assets based upon their classification and priority
    - Evaluation and recommendations of the data backup strategy

Cybersecurity Risk Management Process

Protection Strategy

Strategy to protect the Crown jewels

- Objective - Walk through the NIST Cyber Security Framework category by category and evaluate the potential deployment within the organization
- Target Audience – IT lead and key team members
- Process - Facilitated session
- Deliverable – Feedback on the current state of the cyber security readiness of the organization as well as recommendations on building a robust Cyber Security Program

Cybersecurity Risk Management Process

Protection Build

Deployment of protection strategies

- Objective – Deploy the controls identified to protect
- Target Audience – Assigned IT resources
- Process – One-on-one support as needed

Cybersecurity Risk Management Process

Policy Development

Build out of policies

- Objective – Build out policies as identified to potentially include:
  - Governance strategy and cyber security program - Cybersecurity policy/IT security policy
  - Data management and protection strategy
  - Risk Assessment
  - Incident Response Plan
  - Business Continuity Plan/Disaster Recovery Plan
  - Vendor Management Process
  - Target Audience – Data owners and IT lead
  - Process – One-on-one support

Why leverage this Framework?

Governance - You decide where you want to end up on the security continuum

Identification - You determine what your crown jewels are

Risk Assessment - You assess your risk to the crown jewels

Backup strategy - You determine the appropriate backup cycle for your crown jewels

Business Impact - You determine the important processes to sustain your business in the event of disruption

Protection Strategy - You determine the appropriate strategy to protect your crown jewels

Policy Development - By first determining your governance strategy, identifying your crown jewels and determining how to protect them, you will create a comprehensive set of policies communicate your strategy

Making the complex, simple!

Contact Us

Jim Carpp

Chief Digital Officer
james.carpp@rehmann.com

Jim Bruxvoort

Director of Partnered Technology Services
jim.bruxvoort@rehmann.com

QUESTIONS