Risk Cooperative

CYBER 360°

Your Strategy for Cyber Recovery

Presented by:

INFRAGARD MEMBERS ALLIANCE NEW YORK METRO

INFRAGARD 25 YEARS PARTNERSHIP FOR PROTECTION

About Risk Cooperative

A key focus area for Risk Cooperative is emerging risks, cyber being the top concern.

- Founded in 2014
- Robust employee benefits practice, including group disability, key life and retirement planning
- Extensive expertise across all classes of insurance including, life, health, property, casualty, specialty risks as well as excess and surplus lines of insurance
- Licensed nationally across all 50 states, Puerto Rico and Washington, D.C.
- Global coverage capabilities
- Offices in Washington D.C.

Agenda

01 Anatomy of a Breach

02 Building Response Plans

03 Identifying Cyber Risks

04 Quantifying Cyber Risks

05 Questions?

01 Cyber Risk: Threat Actors, Motivations, and Goals

There are several types of threat actors that organizations must contemplate when assessing cyber risks and developing recovery strategies. This list looks at malicious threat actors as these are the threat verticals which are often hardest to mitigate against.

Threat Actor	Motivations	Goals	Examples
Nation-states, proxy groups	Geopolitical, Ideological	Disruption, destruction, damage, theft, espionage, financial gain	• Permanent data corruption • Targeted physical damage • Power grid disruption • Payment system disruption • Fraudulent transfers • Espionage
Cybercriminals	Enrichment	Theft/financial gain	• Cash theft • Fraudulent transfers • Credential theft
Terrorist groups, hacktivists, insider threats	Ideological, discontent, grudge	Disruption	• Leaks, defamation • Distributed Denial of Service (DDoS) attacks

01 Need For Cyber Recovery Plans

Colonial Pipeline, one of the nation's biggest fuel pipeline operators suffered a ransomware attack forcing it to shut down its entire network on Friday 5/10/21.

The attack appears to have been carried out by an Eastern European-based criminal gang — DarkSide, according to a U.S. officials.

This is the latest in a long list of attacks aimed at critical infrastructure.

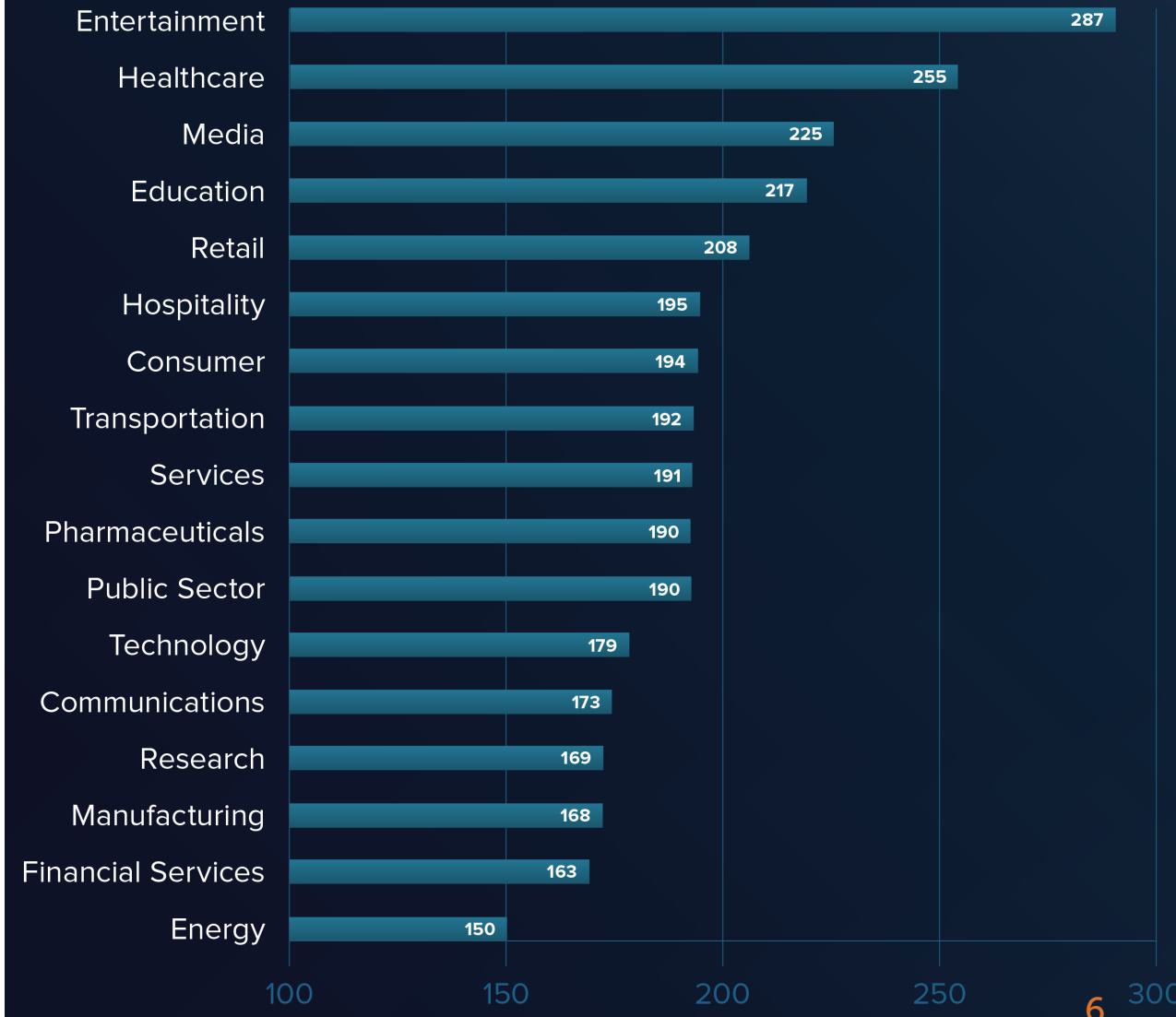
It highlights the real threat that cyber attacks pose to organizations of all sizes and sectors.

It also highlights the need for pro-active cyber preparedness and risk mitigation strategies.

01 Anatomy of a Breach

- The cost of a breach can go beyond the amount of data lost or disclosed depending on the time it takes to find it.
- On average, companies take about 197 days to identify and 69 days to contain a breach according to IBM.
- The longer the breach stays undetected, the costlier it can become.
- Companies that contain a breach in less than 30 days save more than $1 million in comparison to those who take longer.
- Regulatory fines can be another cost driver as companies can face major fines if they take too long to disclose a breach or notify impacted parties.
- According to IBM the cost alone of notifying customers about a hack averages about $740,000 in the United States.

Average Number of Days to Detect Breach by Industry



Source: IBM

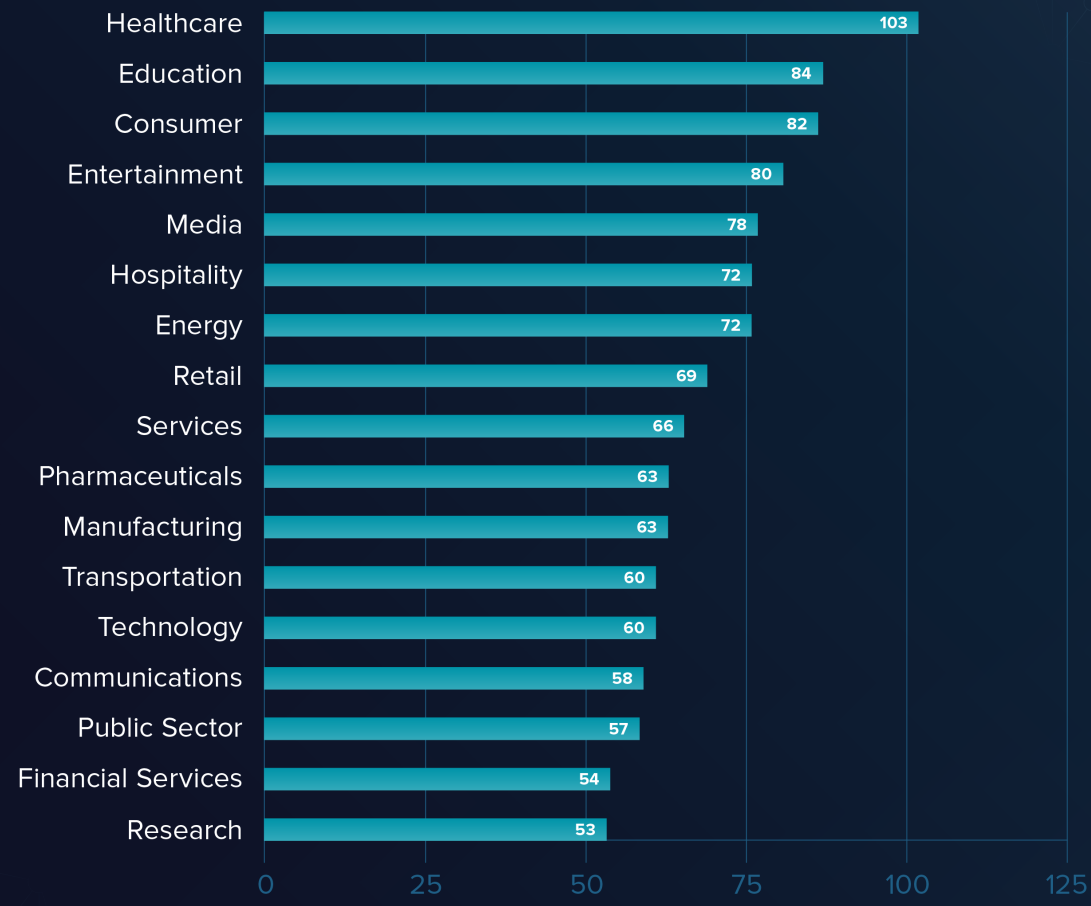
01 Anatomy of a Breach

The average time to contain a breach, on the other hand, is significantly less on average than the time it takes to identify the breach.

Healthcare tops the list, taking 103 days to contain a breach while the research industry takes only 53 days.

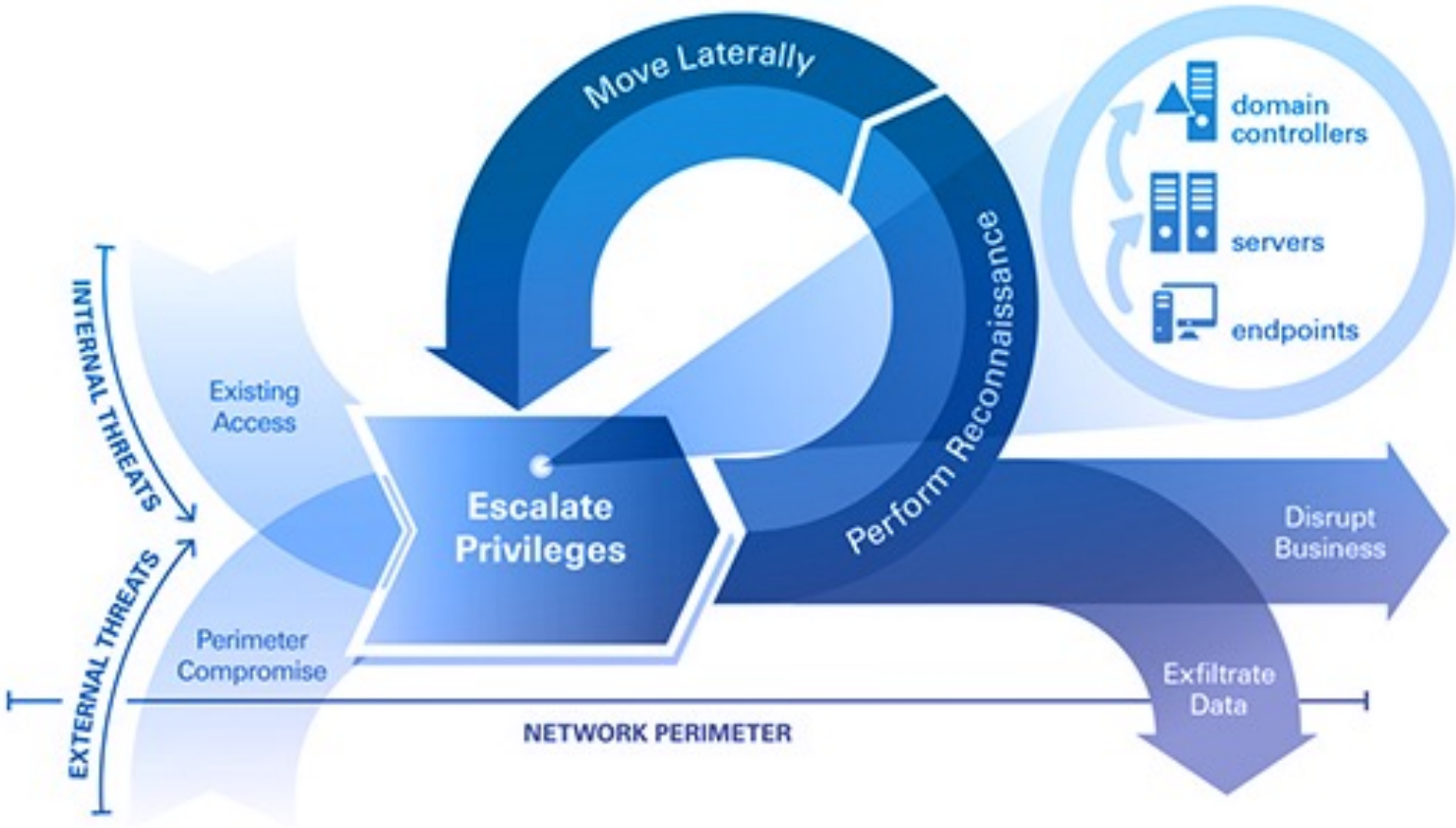
Technology is tool that can help expedite response time and reduce costs, especially automation.

Average Number of Days to Contain Breach by Industry



Source: IBM

01 Anatomy of a Breach



- Motivated attackers will find a way to break through the network perimeter.
- Research findings show that in most attack scenarios, there is a clear attack path that cyber criminals follow to help them remain undetected for extended periods of time.
- Privileged accounts are at the center of this path.

02 Key Mitigation Steps

These 6 key mitigation steps will help provide a roadmap for quicker response time and recovery in the event of a cyber incident.

Incident Response & Resiliency Policies, Procedures & Plans

Assessing, testing, and periodically updating incident response and resiliency policies and procedures

Operational Resilience

Identifying business and operational disruption scenarios and their recovery strategies

Awareness & Training

Developing appropriate security awareness content and providing cybersecurity and resiliency training to employees, contractors and third parties

Access Management

Developing a comprehensive user access management program, policies and procedures

Perimeter Security

Identifying and implementing network security solutions including network & email traffic monitoring and analytics, as well as other advanced solutions such as intrusion detection and prevention

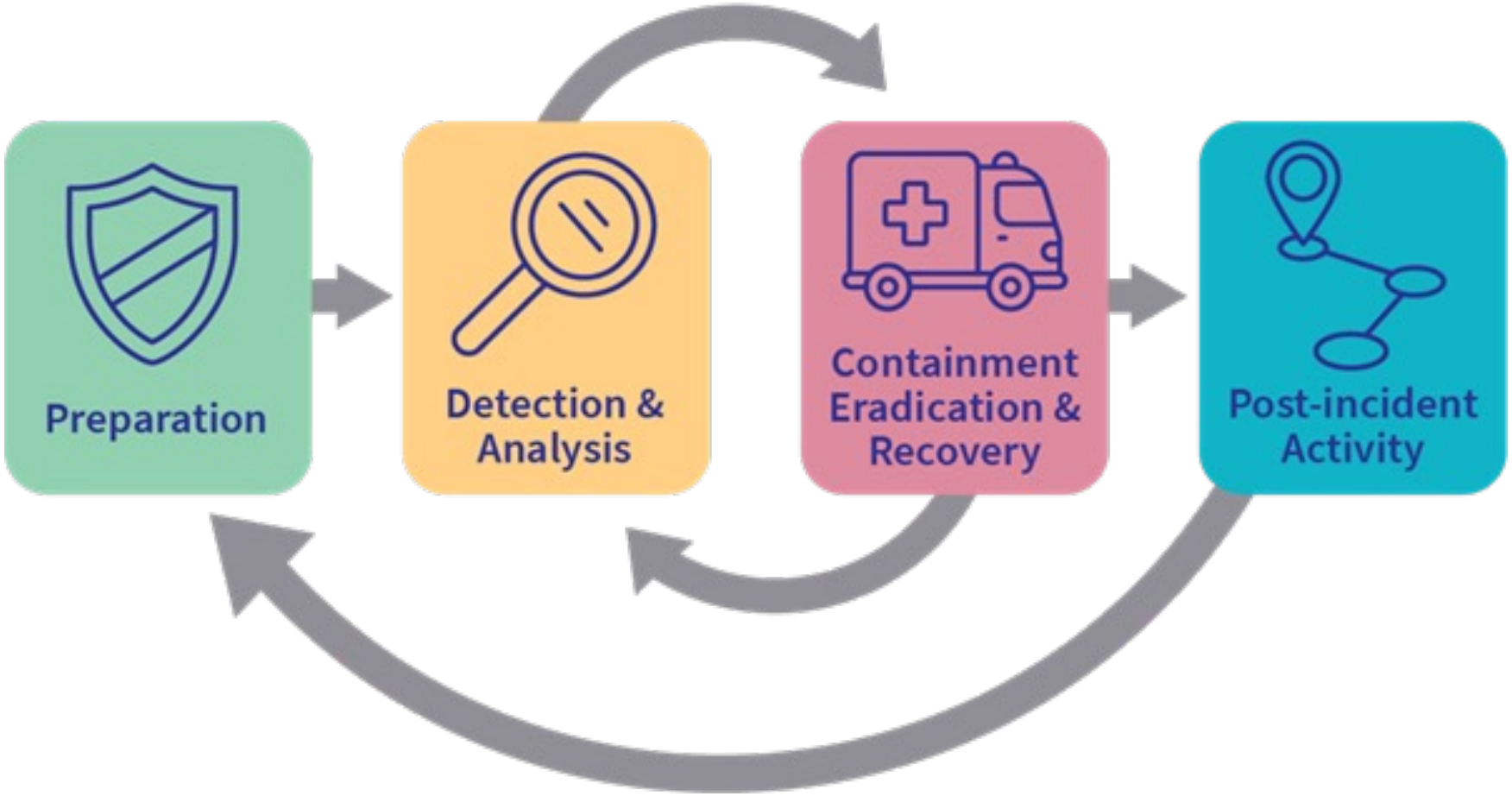
Vulnerability Scanning and Patch Management

Developing proactive vulnerability and patch management programs that are commensurate with the evolving threats & risks

02 Key Response Trends

- Companies with dedicated, trained teams and tested response plans can respond faster.
- Preparation, technology and adherence to privacy laws all make a notable impact for a company's response time.
- Security automation decreases the average response time.
- It's faster to contain a breach caused by human error versus a breach caused by malicious attacks.
- The faster the data breach is identified and contained, the lower the costs.
- The more barriers and precautions you can put in place between data and the hacker, the longer you have to find threats.
- Preparation and tested response plans also speed up response times to stop hackers before any more damage occurs.

02 Developing a Response and Recovery Plan



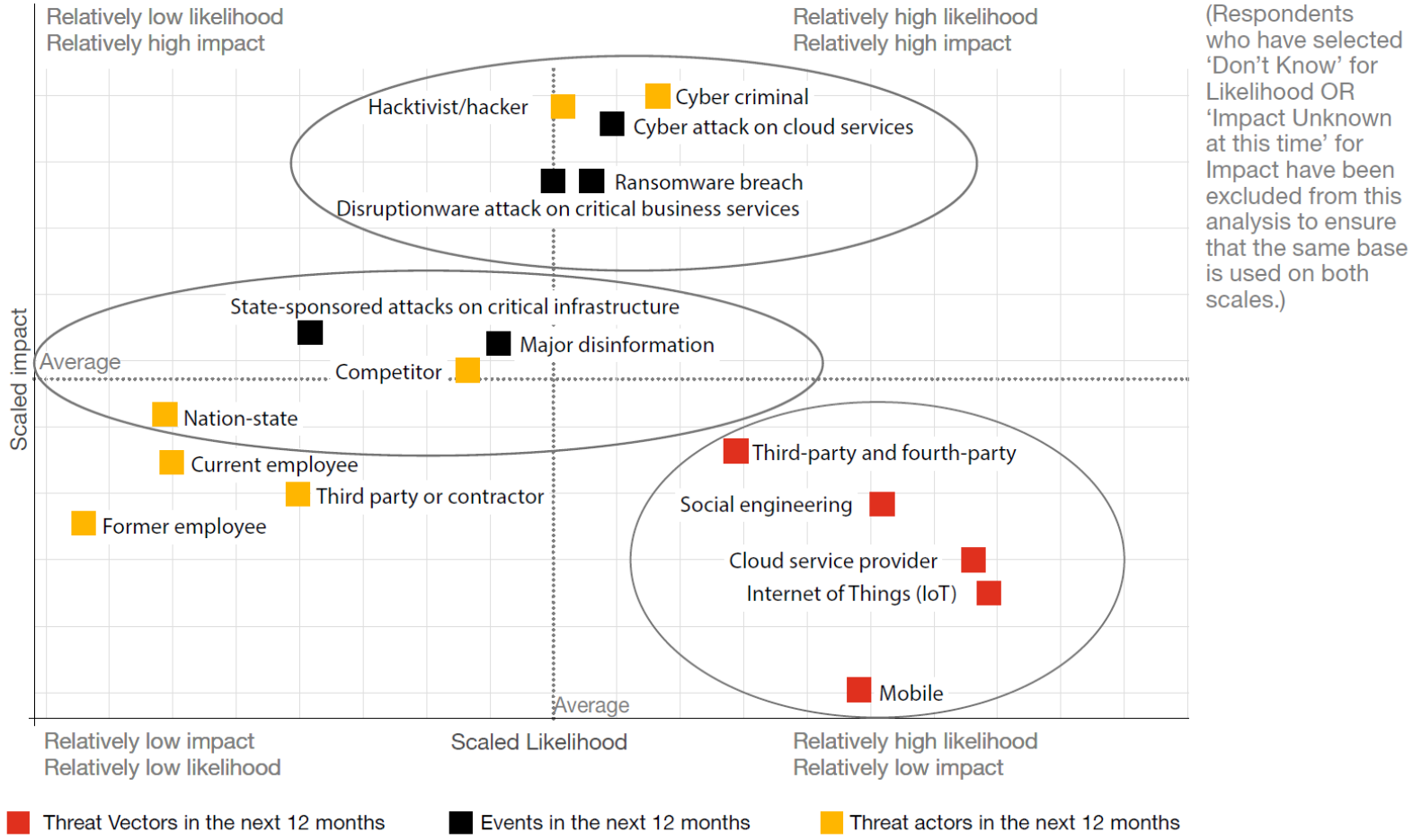
02 Building Your Cyber Framework

Function	Category	The Challenge	Physical Controls	Cyber Controls
Identify	Asset Management	What processes and assets need protection?		
	Business Environment			
	Governance			
	Risk Assessment			
	Risk Management Strategy			
	Supply Chain Management			
Protect	Access Control	What safeguards or countermeasures are available?		
	Awareness and Training			
	Data Security			
	Info Protection Process & Procedure			
	Maintenance			
	Protective Technology			
Detect	Anomalies and Events	What techniques can identify cybersecurity incidents?		
	Security Continuous Monitoring			
	Detection Processes			
Respond	Response Planning	What activities can contain impacts of incidents?		
	Communications			
	Analysis			
	Mitigation			
	Improvements			
Recover	Recovery Planning	What activities are required to restore capabilities?		
	Improvements			
	Communications			

- To build a proper response, organizations must first understand their current operating environments.
- Frameworks should look at all areas of the organization to identify what controls are needed and the proper mitigation strategies.
- Protection levels will help determine the type of investments, and assets the organization should prioritize.
- Ongoing surveillance and detection helps to ensure that any outlier behavior is quickly reported.
- All segments help inform the response and recover phases to help minimize downtime and expedite recovery of operations.
- All functions should be performed concurrently as cyber is a dynamic risk.

03 Risk Assessment

Threats, actors, and events: relative likelihood and impact



Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,217

- Response is critical, but it is also necessary to understand the likelihood and impact any potential threat may have on an organization.
- This enables organizations to determine the best response and mitigation strategy.
- PWC's survey showed key metrics from its Trust Insights survey of corporations.
- IoT and cloud service providers top the list of 'very likely' threat vectors (mentioned by 33%)
- Cyber attacks on cloud services top the list of threats that will have 'significantly negative impact' (reported by 24%).

03 Risk Identification

- The primary goal in identifying risks is to produce a comprehensive list of risks and to assess them, narrowing the list down to the most critical risks facing the organization.
- At the conclusion of the risk identification process, the company should be able to identify those risks that will have the greatest likelihood of occurring and the potential impact to the organization.
- Developing heat maps is a useful way to help organizations better quantify the potential risks and rank them accordingly.

Impact

Likelihood / Risk Matrix	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Medium	Medium	Medium High	High	High
Likely	Low	Low Medium	Medium	Medium High	High
Possible	Low	Low Medium	Medium	Medium High	Medium High
Unlikely	Low	Low Medium	Low Medium	Medium	Medium High
Very Likely	Low	Low	Low Medium	Medium	Medium

03 Risk Ranking and Classification

Risk ranking and classification process is another way for organizations to further enhance their defenses.

The ranking and categorization process provides critical information to executives as to vulnerabilities and helps inform the necessary investments to safeguard against them.

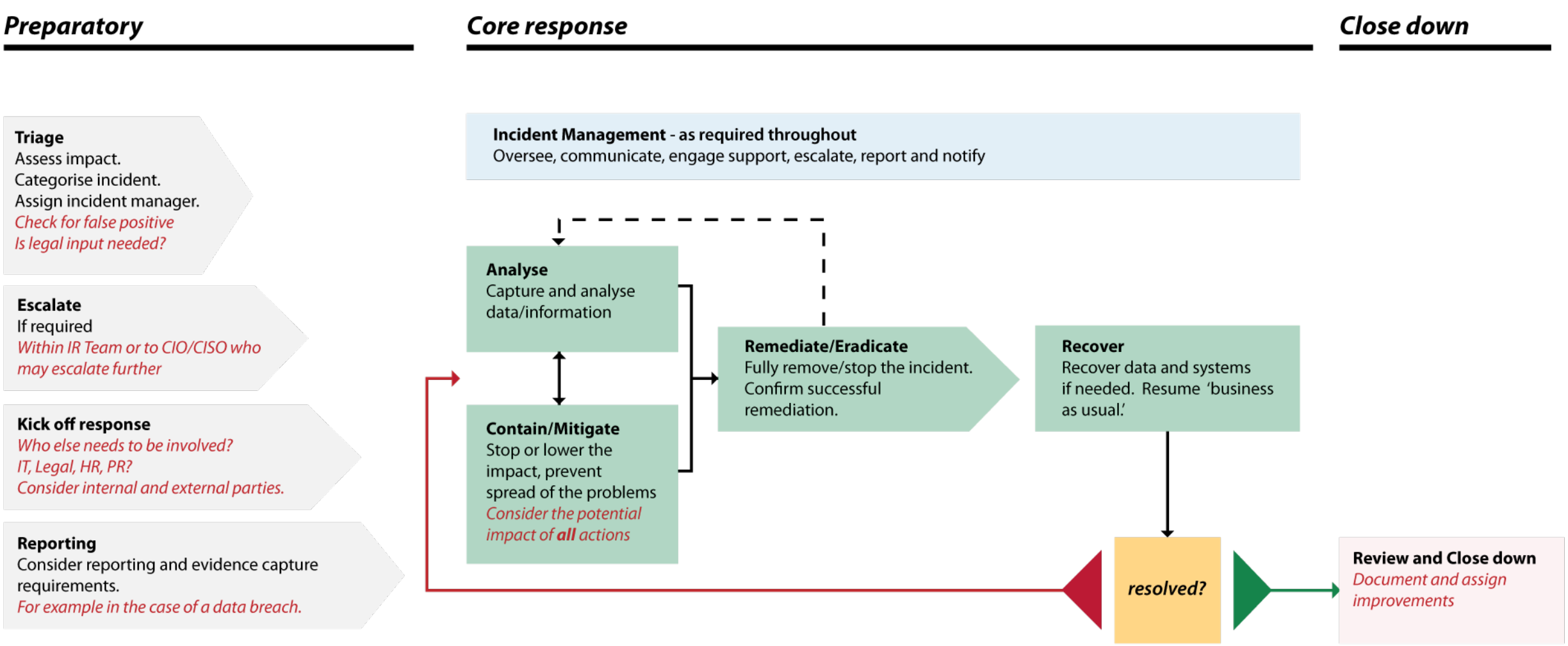
03 Risk Control Strategies

The final stage in the assessment process, is to identify and determine the necessary risk control treatment. The standard models or risk controls include:

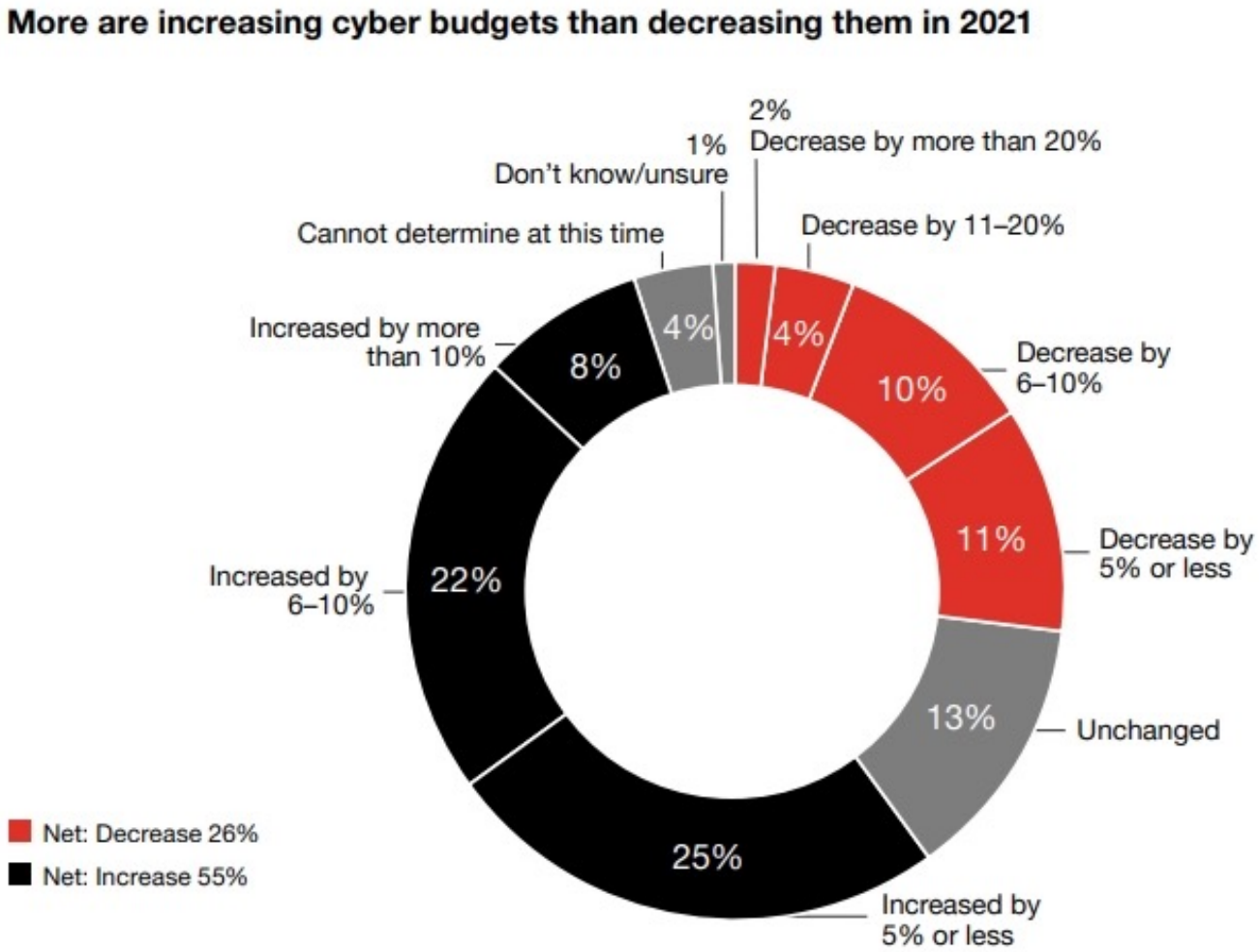
- Avoidance
- Reduction
- Sharing
- Acceptance

Threat	Vulnerability	Asset and consequences	Risk	Solution
System failure — overheating in server room **High**	Air conditioning system is ten years old. **High**	Servers. All services (website, email, etc.) will be unavailable for at least 3 hours. **Critical**	**High** (potential loss of $50,000 per occurrence)	Buy a new air conditioner (cost: $3,000)
Malicious human (interference) — distributed denial-of-service (DDoS) attack **High**	Firewall configured properly and has good DDOS mitigation. **Low**	Website. Website will be unavailable. **Critical**	**Moderate** (potential loss of $5000 per hour of downtime)	Monitor firewall
Natural disaster — flooding **Moderate**	Server room is on the 3rd floor. **Very low**	Servers. All services will be unavailable. **Critical**	**Very low**	No action needed
Accidental human interference — accidental file deletions **High**	Permissions are configured properly; IT auditing software is in place; backups are taken regularly. **Low**	All files on a file share. Critical data could be lost, but almost certainly could be restored from backup. **Moderate**	**Low**	Continue monitoring permissions changes, privileged users, and backups

03 Recovery Plan in Action



04 Investing in Cybersecurity

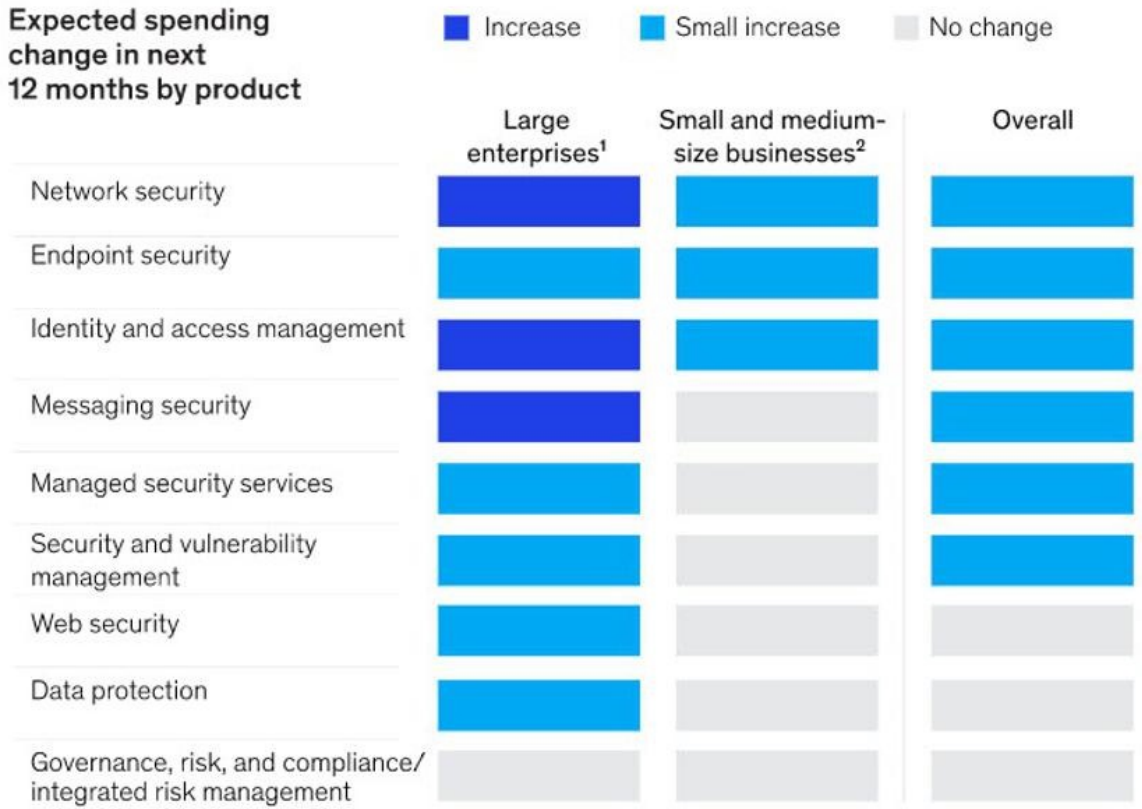


Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: How is your cyber budget changing in 2021? base 1,414

Given increased cyber attack trends, most corporations are increasing cybersecurity budgets. According to PwC's 2021 Global Digital Trust Insights report, 96% of business and technology executives prioritized their cybersecurity investments. In 2019, that figure was closer to 25%.

04 Technology Spend Does Not Equal Security

- Majority of organizations, both large and small, are focusing on tech driven solutions.
- Yet, more than half (55%) of business and tech/security executives lack confidence spend is aligned to the most significant risks.
- Or that their budget funds remediation, risk mitigation and/or response techniques that will provide the best ROI (55%).
- Or that the process monitors the cyber program's effectiveness compared to expenditures (54%).
- And with regard to preparedness for future risks, executives are not confident that cyber budgets provide adequate controls over emerging technologies (58%).
- Greater focus on governance and risk management needs to be integrated into recovery and preparedness plans if organizations want to increase their overall resiliency to attacks.

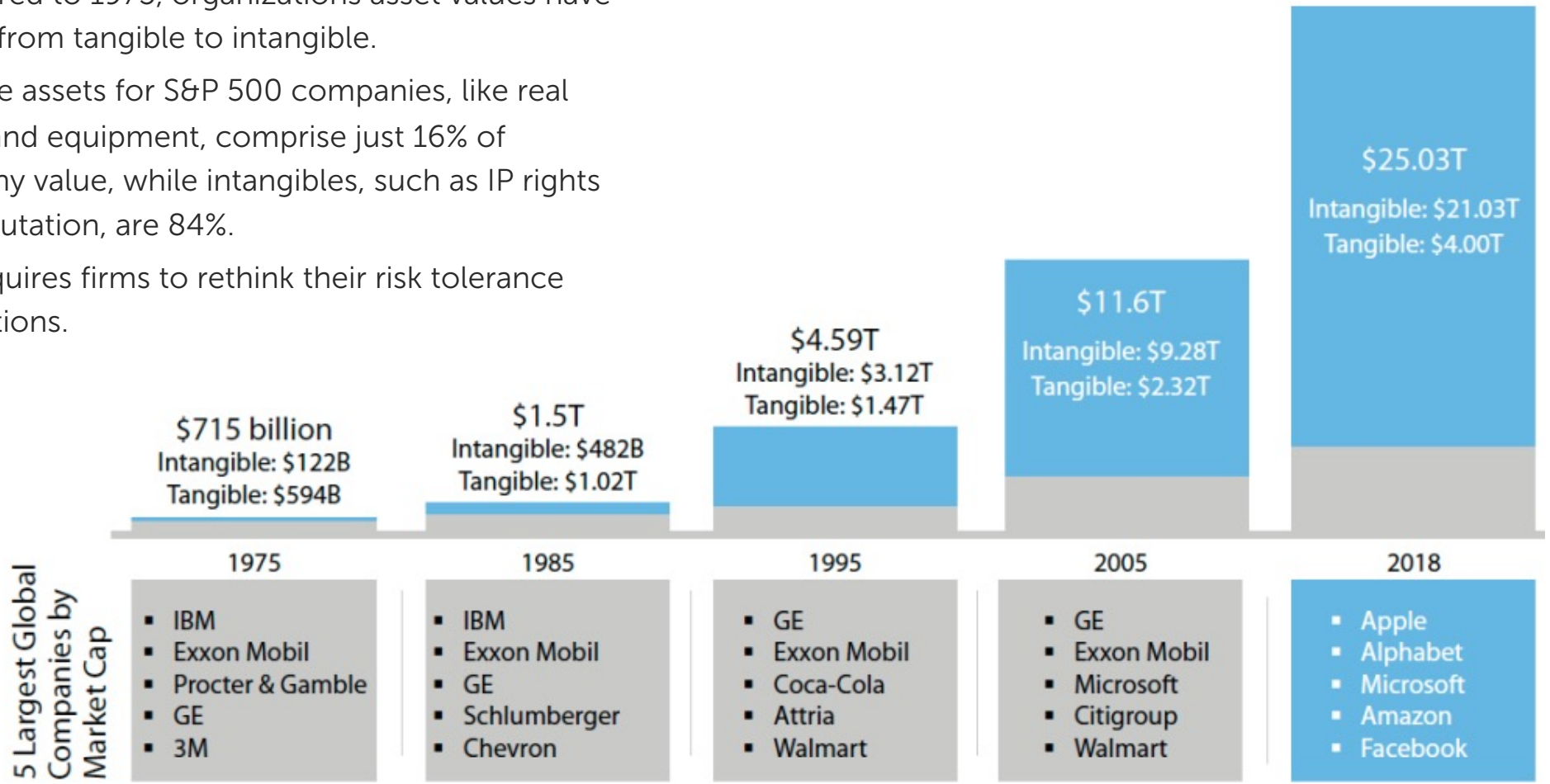


- >70% of CISOs[3] and security buyers believe budgets will shrink by end of 2020 but plan to ask for significant increases in 2021
- Product spending reflects CISOs' need to address pandemic-era business conditions, including safeguarding remote workers from heightened attacks

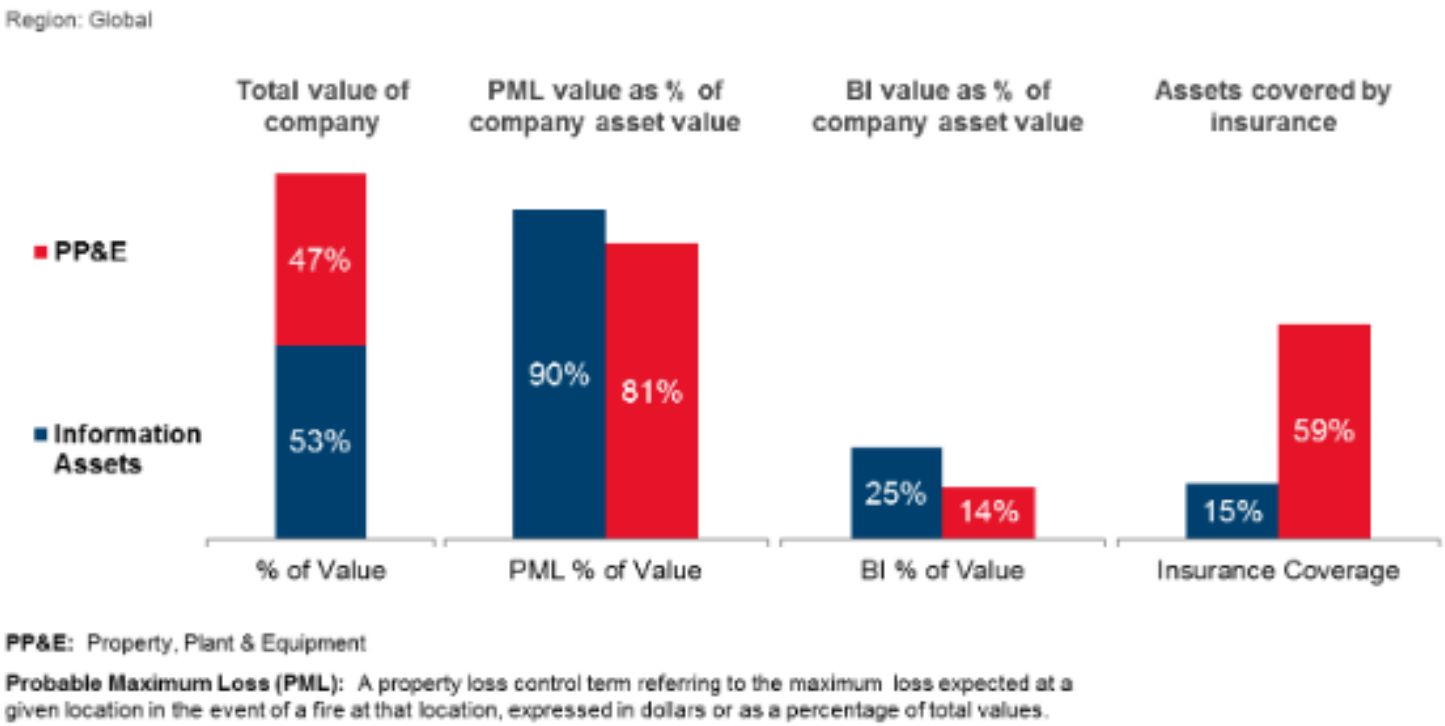
[1]>5,000 employees.
[2]<5,000 employees.
[3]Chief information-security officers.
Source: Expert interviews; McKinsey analysis

04 Risk and Asset Quantification

- Compared to 1975, organizations asset values have shifted from tangible to intangible.
- Tangible assets for S&P 500 companies, like real estate and equipment, comprise just 16% of company value, while intangibles, such as IP rights and reputation, are 84%.
- This requires firms to rethink their risk tolerance calculations.



04 Know What your Data is Worth

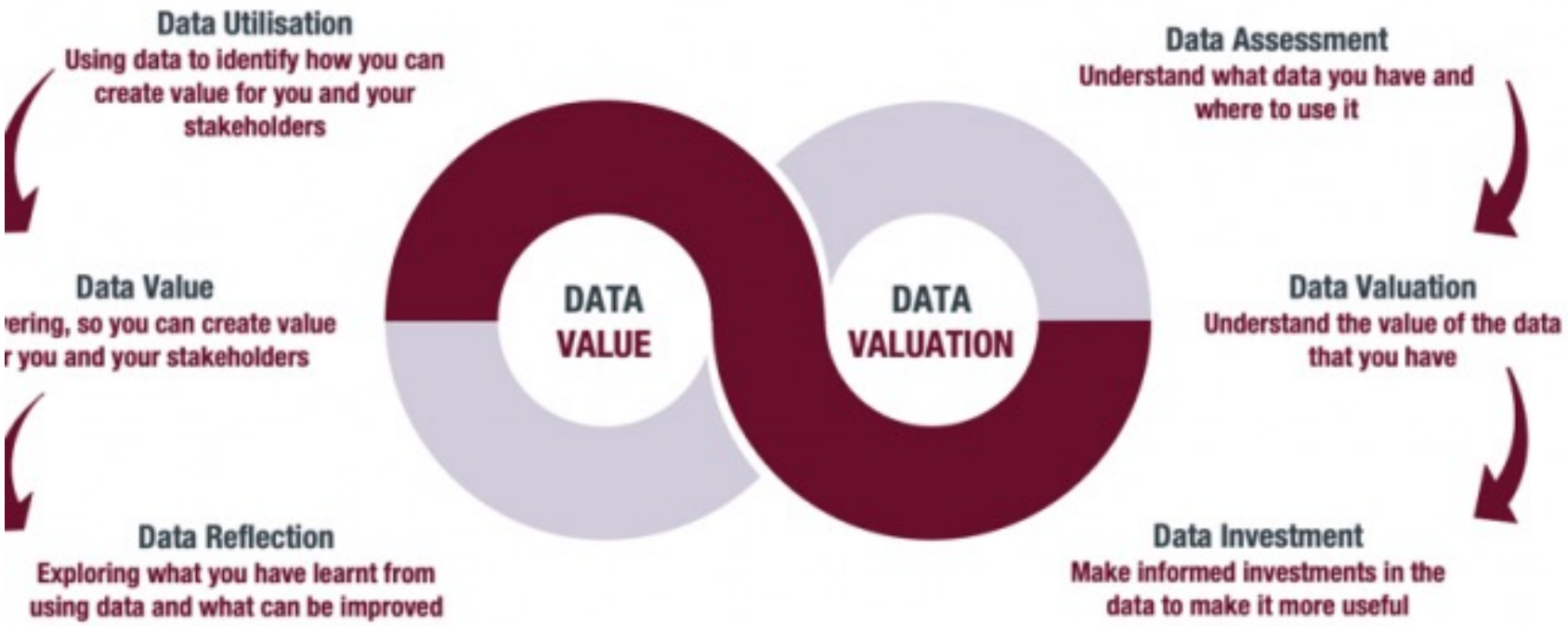


PP&E: Property, Plant & Equipment

Probable Maximum Loss (PML): A property loss control term referring to the maximum loss expected at a given location in the event of a fire at that location, expressed in dollars or as a percentage of total values.

- Cyber risk quantification is not easy and there is not yet a standardized model for best approach.
- It requires understanding the types of data and assets in an organization.
- Organizations have long focused on the cost side of cybersecurity - compliance, updating capabilities, and so on.
- Many companies do not realize their information assets are their most asset, yet remain unprotected, uninsured or otherwise at risk.
- Executives who begin to quantify their cyber risk and digital assets are realizing benefits such as:
  - M&A deal evaluation and cyber liability protections.
  - Protected IP and contract values.
  - Accurate insurance business income protections.
  - Better risk control performance monitoring and threat assessment capabilities.

04 Economic Value of Data



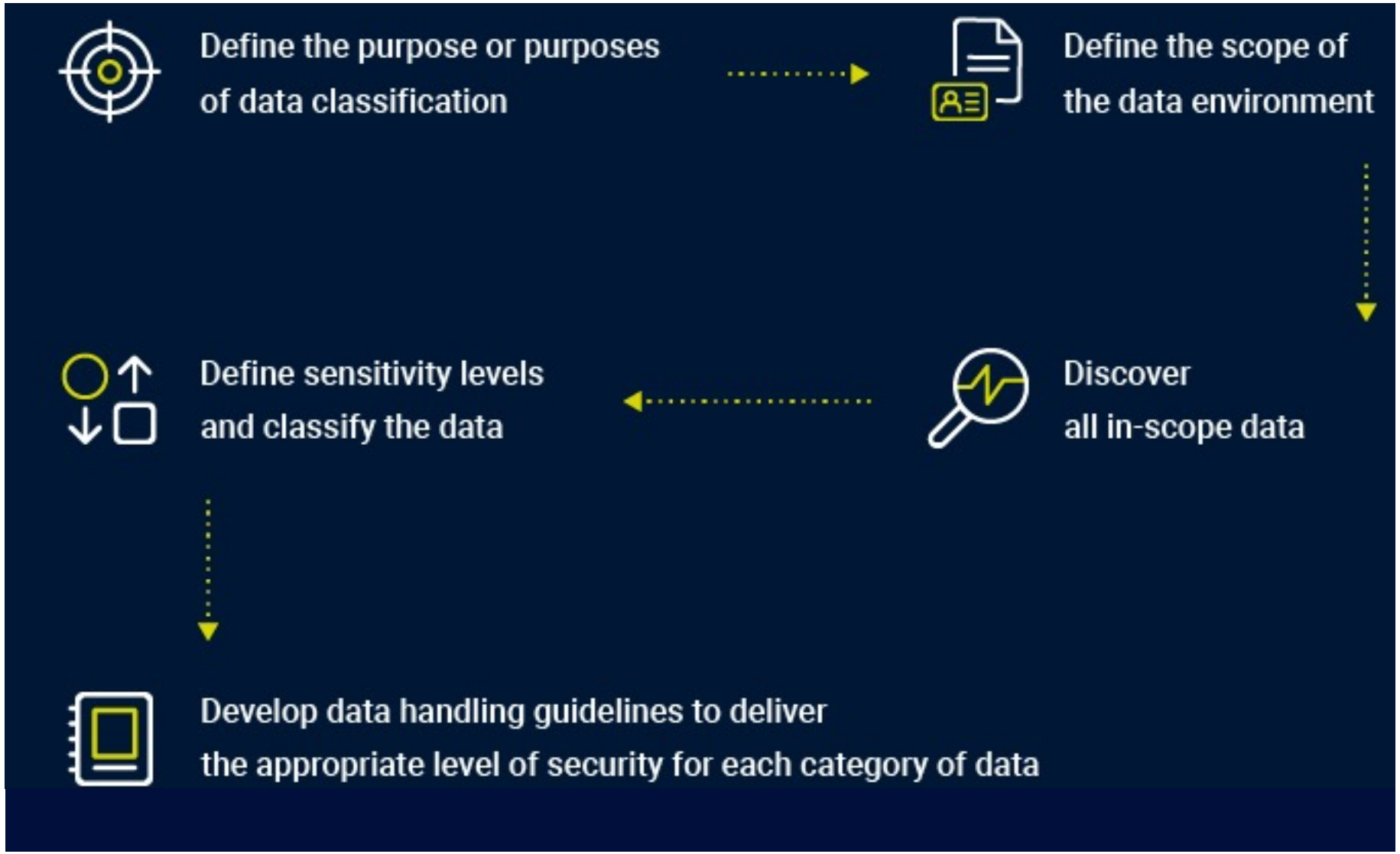
- Not all data is created equal.
- As Big Data continues to take over, data is becoming more and more of an asset, an asset that grows in value through use.
- Understand the value of your data will help inform how best to protect it and how to insure it against its cyber risk.
- Some firms have a lower data value than others – for example CSX has a lower comparative data valuation than Google.
- This must factor into an organizations overall strategic plans.

04 Data Classification

Sensitivity	Definition	Information and Data Sensitivity Classification
Low or No	Information or data that, if disclosed or accessed without proper authorization, are unlikely to cause any harm or negative impacts to affected people and/or humanitarian actors.[5]	**Public**
Moderate	Information or data that, if disclosed or accessed without proper authorization, are likely to cause minor harm or negative impacts and/or be disadvantageous for affected people and/or humanitarian actors.	**Restricted**
High	Information or data that, if disclosed or accessed without proper authorization, are likely to cause serious harm or negative impacts to affected people and/or humanitarian actors and/or damage to a response.[6]	**Confidential**
Severe	Information or data that, if disclosed or accessed without proper authorization, are likely to cause severe harm or negative impacts and/or damage to affected people and/or humanitarian actors and/or impede the conduct of the work of a response.[7]	**Strictly Confidential**

- Companies must know the type of data they are storing, as well as its value to the organization.
- Only then can they develop a proper classification and protection system.
- Putting data classification at the heart of your data protection strategy allows you to reduce risks to sensitive data, enhance decision-making and increase the effectiveness security controls.
- This ultimately helps the organization remain resilient and protects its key digital assets.

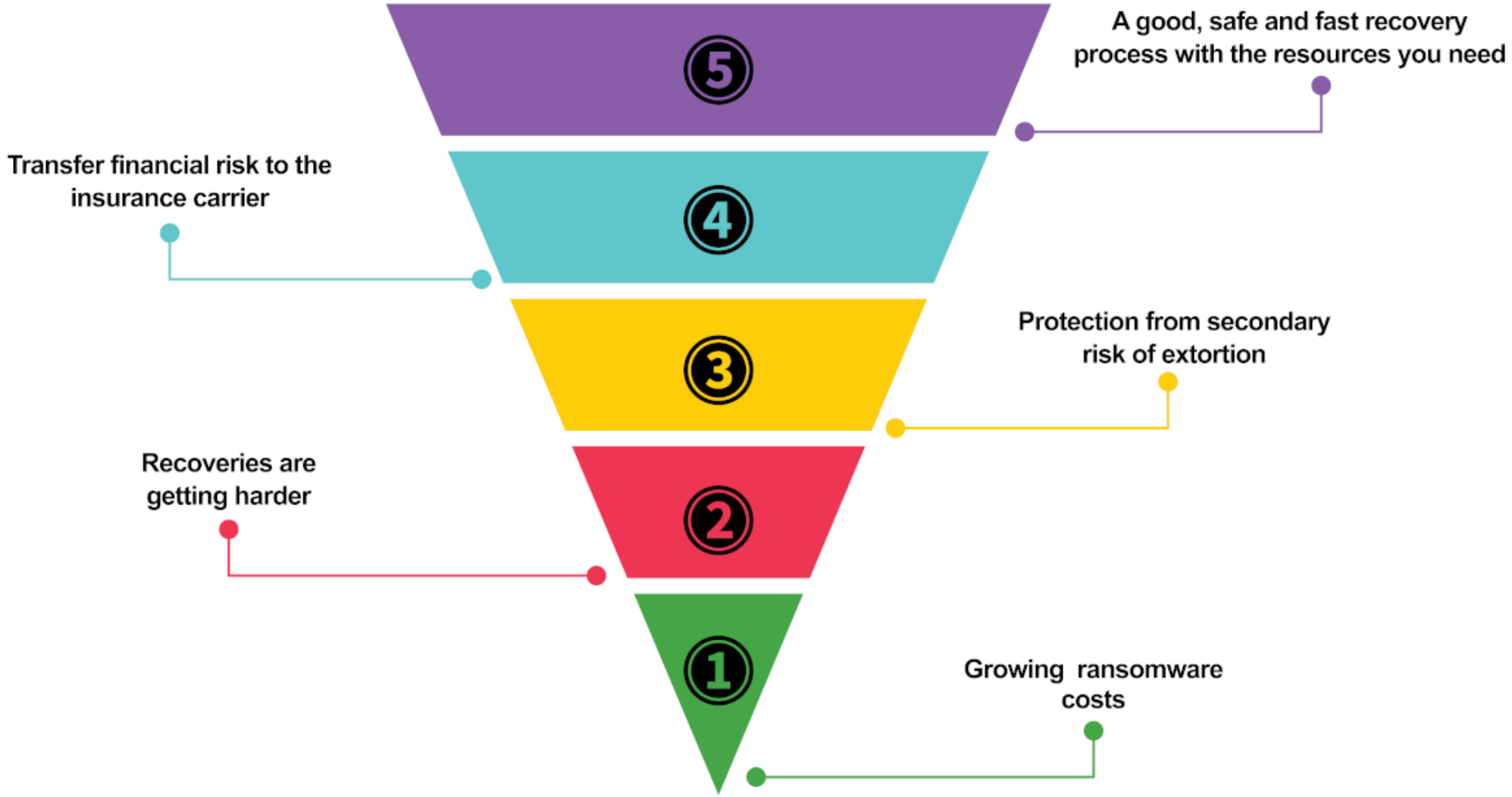
04 Data Classification Process



04 Data Classification By Compliance Standard

NIST 800-53	To identify how to maintain systems, applications and integrations in order to ensure data confidentiality, integrity and availability
ISO 27001	To comply with industry standards that require data to be classified
HIPAA	To inventory ePHI and identify risks to its confidentiality, availability and integrity
PCI DSS	To mitigate the risk of unauthorized disclosure and access
GDPR	To satisfy data subject access requests by retrieving all information about an individual in the required timeframe

04 Five Reasons For Cyber Insurance



04 10 Steps to Cybersecurity

Network Security
Protect your networks against external and internal attack.
Menage the network perimeter. Filter out unauthorised access & malicious content. Monitor & test security controls.

User education and awareness
Produce user security polices covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls
Produce a policy to control all access to removable media.Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges
Establish effective managemant processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

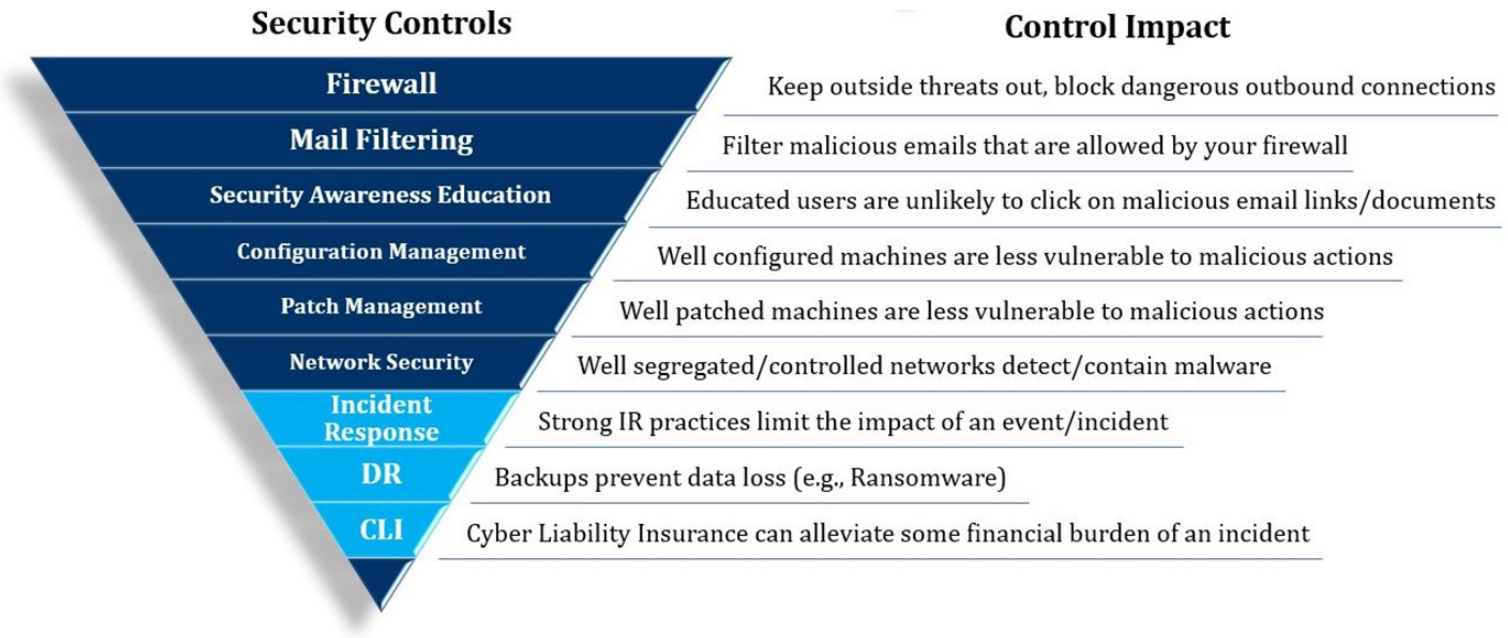
Incident management
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

04 Key Focus Areas

Cybersecurity can be overwhelming, however there are key areas to start that provide demonstrable ROI for risk mitigation.



Incident response: Even with robust network security in place, an incident response (IR) plan is still required to minimize the potential impact. This provides an organized, coordinated response as well as early detection.

Disaster recovery/backup: Having up to date backups offsite, can allow you to regain control and resume operations in the face of would-be ransomware attacks.

Cyber insurance: Cyber insurance allows organizations to transfer the financial impact of a cyber attack to the insurance company. It also provides breach response resources that will help get the organization back to operations. While it is not a protection against cyber attacks, insurance can build resiliency and absorb both regulatory and third part costs as well as potential income disruptions or reputation damage incurred by a cyber attack.

04 Key Post Breach Actions

Communication

Both **internal** (inform employees and involve everyone able to help, i.e. tech specialist, client service managers, PR & communication team, etc.) and **external** (direct mailing to the clients, official media release - and, if necessary, also interview to the profile press).

Root Cause

Engineers can use forensics to analyze traffic and instantly determine the root cause of an event, entirely removing guesswork and problem reproduction from the equation.

Forensics

Effective forensics provide these four key capabilities:

- **Data Capture:** Capture all traffic, 24x7, on even the fastest links
- **Network Recording:** Store all packets for post-incident, or forensic analysis
- **Search and Inspection:** Enable administrators to comb through archived traffic for anomalies and signs of problems
- **Reporting:** Through data capture and analysis, results of investigations are logged, and network vulnerabilities are reviewed and analyzed post-mortem.

Training

Train and learn from the Incident. Reviewing what occurred and training employees to prevent future scenarios is another critical component to building cyber resiliency.

04 Enterprise Risk Management

GOVERNANCE & CULTURE

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops and Retains Capable Individuals

STRATEGY & OBJECTIVE-SETTING

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

PERFORMANCE

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

REVIEW & REVISION

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

INFORMATION, COMMUNICATION & REPORTING

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture and Performance

Questions?

Closing Notes

The **360° Cyber Survey** was designed to help business leaders go beyond baseline compliance and technical components to help evaluate their overall business resiliency to cyber threats.

The report not only provides a detailed overview of the responses, but also analysis from cyber and risk experts and actionable recommendations to help guide members through mitigation steps to improve their cyber resiliency.

Take the Cyber 360° Survey

Materials will be available after the session.

An email will be sent with links to access the recording and slides.

More questions? Send us a message and we'll get you the answers you need.

Risk Cooperative

Risk Cooperative
1825 K Street NW, Ste 1000
Washington, DC 20006

info@riskcooperative.com
P | +1.202.688.3560
F | +1 202.905.0308

InfraGard

Jennifer Rothstein
jrothstein@nym-infragard.us

www.nym-infragard.us
www.infragardnational.org