Risk Cooperative

CYBER 360°

Exposing & Mitigating Cyber Vulnerabilities

Presented by:

INFRAGARD MEMBERS ALLIANCE NEW YORK METRO

INFRAGARD 25 YEARS PARTNERSHIP FOR PROTECTION

Agenda

01 About Risk Cooperative

02 Cyber Current State of Play

03 Cyber Threats & Key Trends

04 Risk Mitigation
Strategies & Frameworks

05 Questions?

01

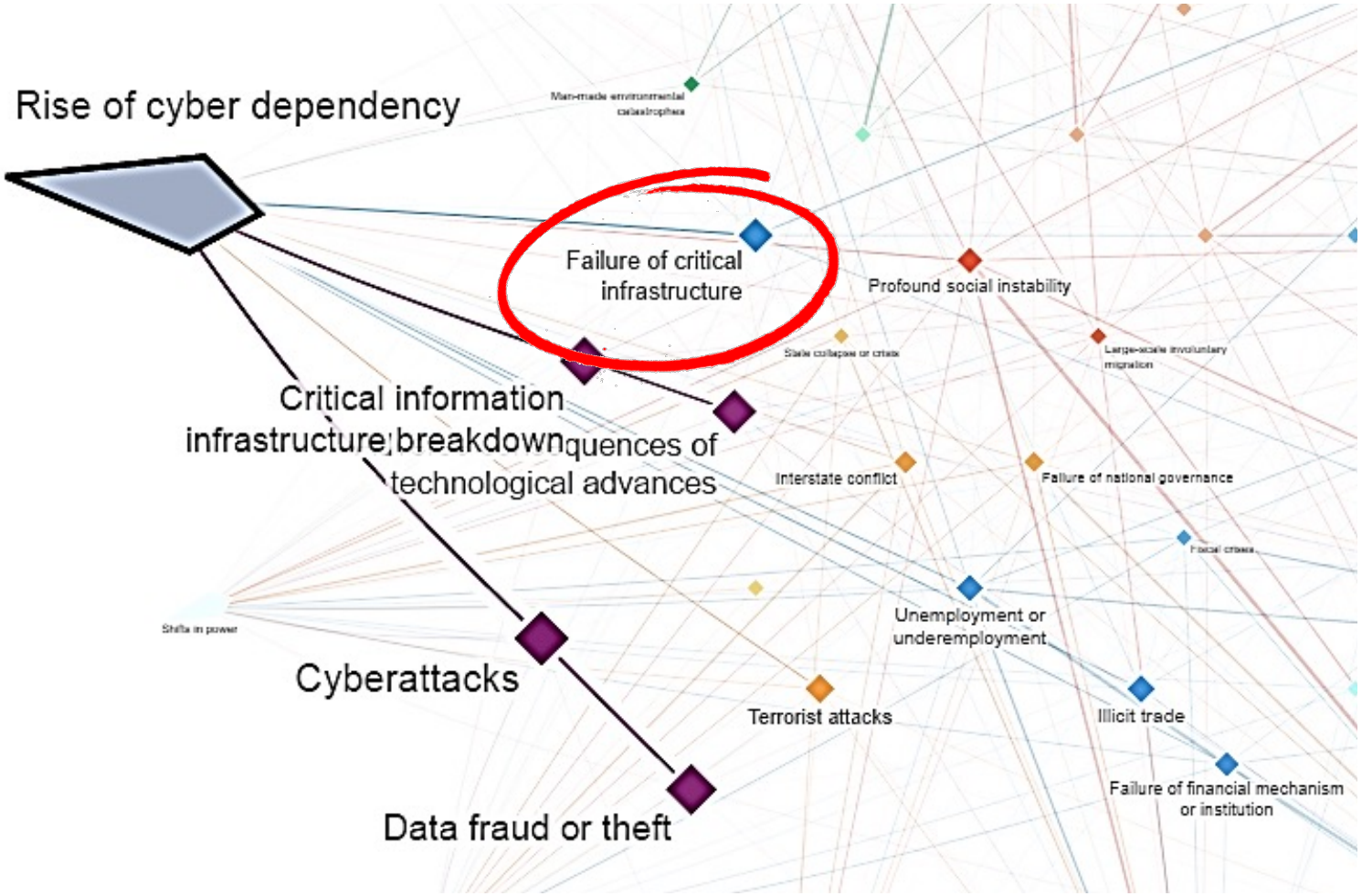
ABOUT

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.

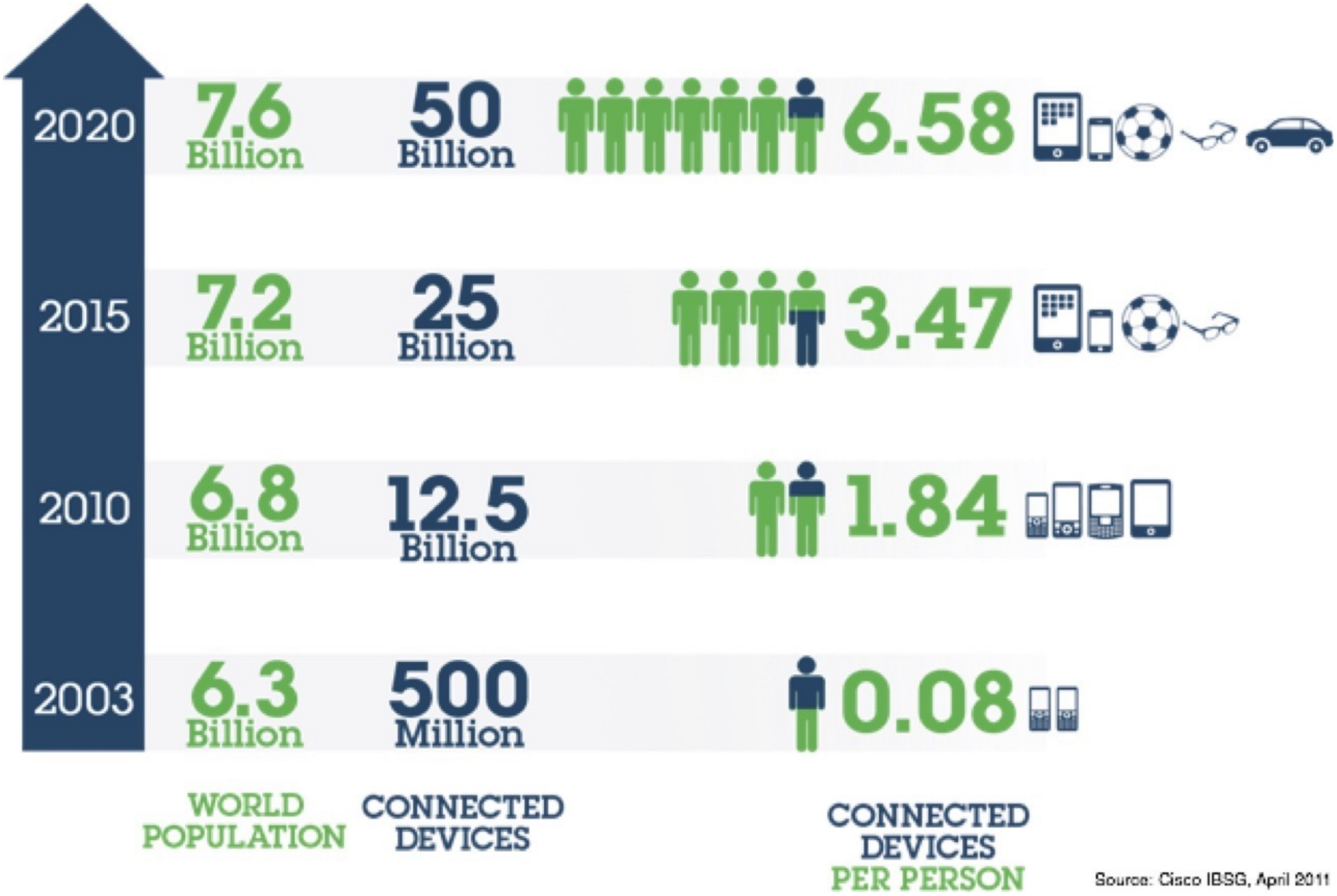
02 Cyber State of Play

CYBER RISK



Cyber risk is increasingly defining the 21st century. Given the systemic connections, virtually every facet of the global economy exposed to this insidious threat.

- As the global economy becomes more technology dependent, cyber attacks have become the new theater of war.
- Cyber attacks are currently considered as being in the top three risks to global economic stability.
- A cyberattack occurs every 39 seconds.
- The rise of "ransomware" and business models being "kidnapped" has been steadily rising with no end in sight.
- WannaCry virus affecting 300,000 organizations in over 150 countries over 3-day span was early indicator of new operating norm.
- No one is "safe" – SolarWinds hack demonstrates even government agencies vulnerable to cyber breaches.


2020
7.6 Billion
50 Billion
6.58
2015
7.2 Billion
25 Billion
3.47
2010
6.8 Billion
12.5 Billion
1.84
2003
6.3 Billion
500 Million
0.08
WORLD POPULATION
CONNECTED DEVICES
CONNECTED DEVICES PER PERSON
Source: Cisco IBSG, April 2011

02

CYBER RISK

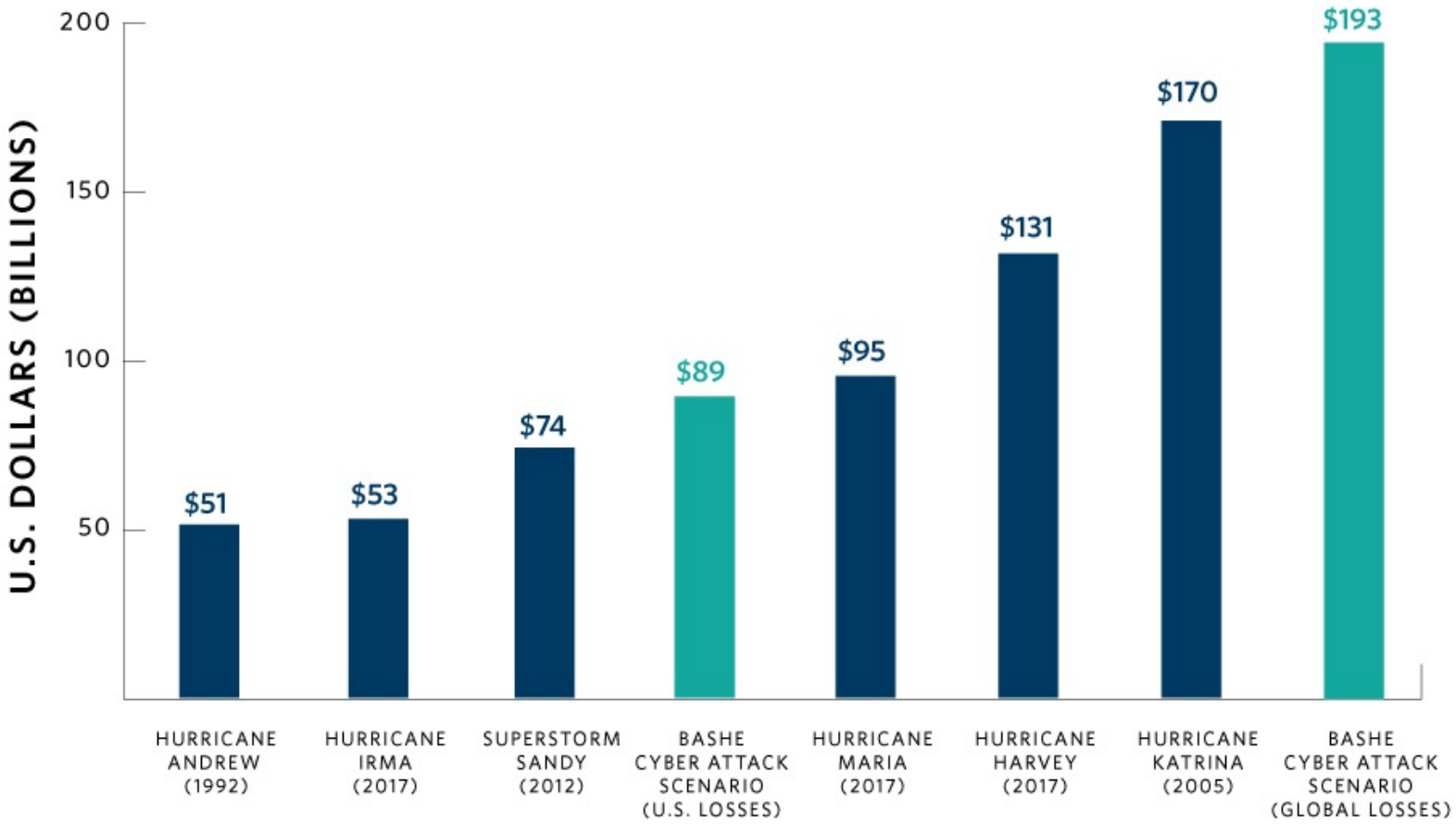
Top Business Risks By Country

Source: Global Risks Perception Survey

02

CYBER RISK

Extreme Cyber Attack vs. U.S. Natural Disasters



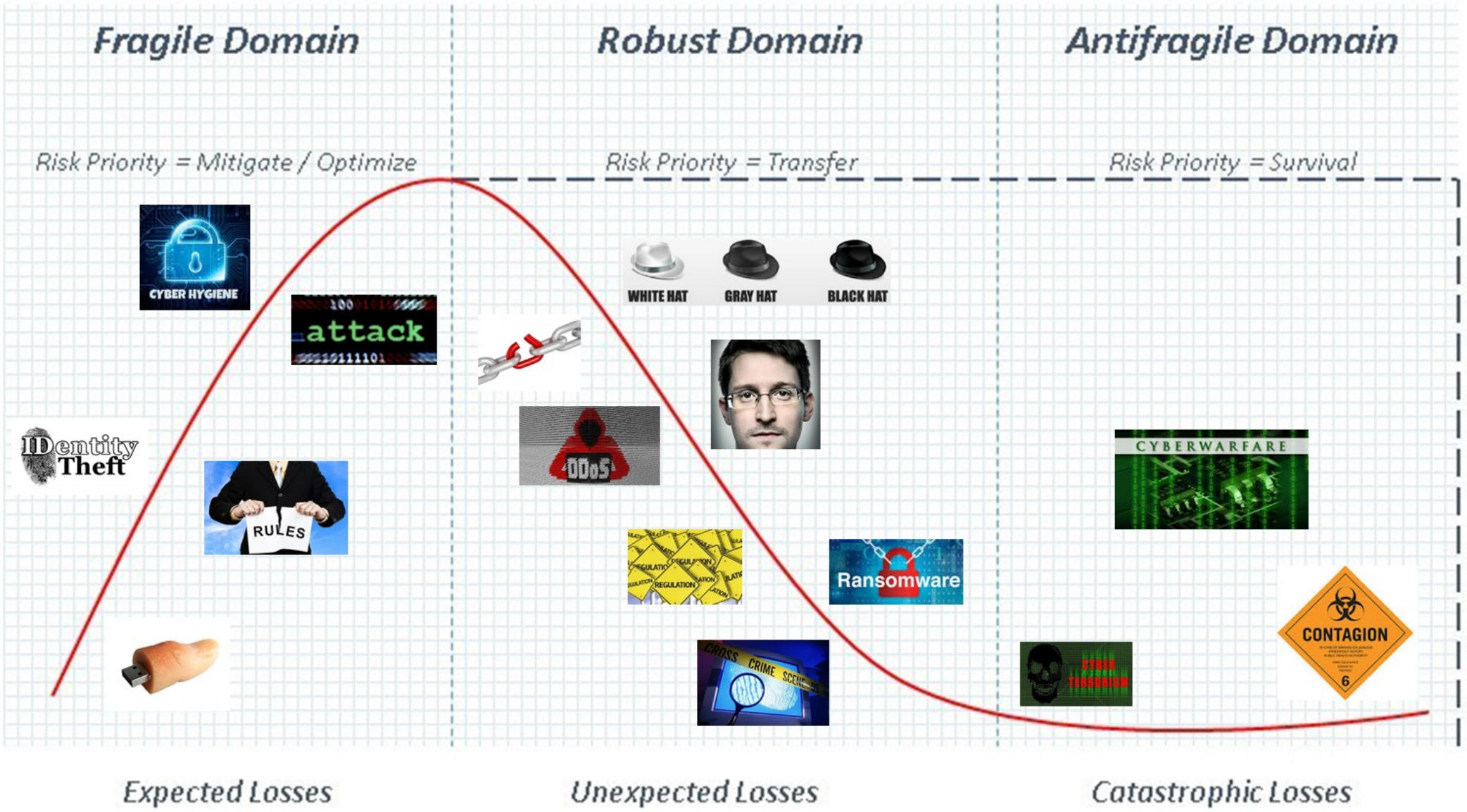
Sources: NOAAA – 2020-Billion-dollar Weather and Climate Disasters Report

The Bashe Cyber Attack study, conducted by Lloyd's of London, where a contagious malware infects large scale company systems, threatening to destroy or block access to files unless a ransom is paid.

Study found the global economy is underprepared for such an attack with 86% of the total economic losses are uninsured ($166bn Gap).

02 Cyber Threat Landscape

CYBER RISK

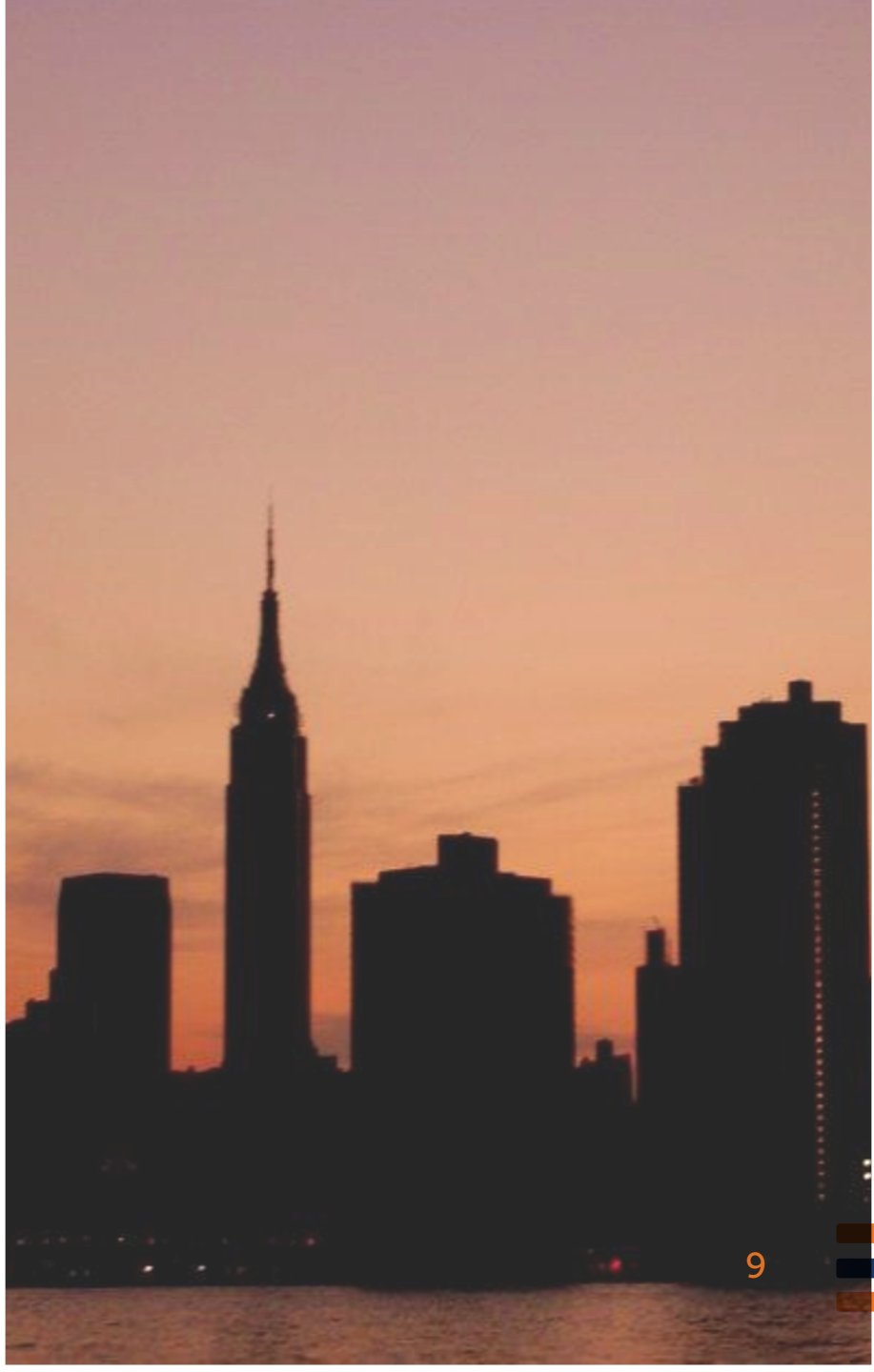


02

CYBER RISK

Critical Infrastructure in the Cross Hairs

- Foreign adversaries are increasing cyber attacks on U.S. critical infrastructure according to the National Security Agency (NSA) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).
- Attacks have been occurring for some time, such as Atlanta's 2018 ransomware attack by Iranian operatives.
- A Siemens/Ponemon Institute study found that 56% of gas, wind, water and solar utilities around the world had experienced at least one cyberattack within the previous year that caused a shutdown or loss of operation data.
- Of the study participants, only 42% indicated high cyber readiness with only 31% stating ability to respond to or contain a breach was high.
- The highly publicized SolarWinds breach, orchestrated by Russia, demonstrate the far reach of these attacks impacting 200 organizations globally, including highly secure US government agencies.



03

RISK

2020 Leading Causes of Breaches

Small vs. Large Company Breach Statistics

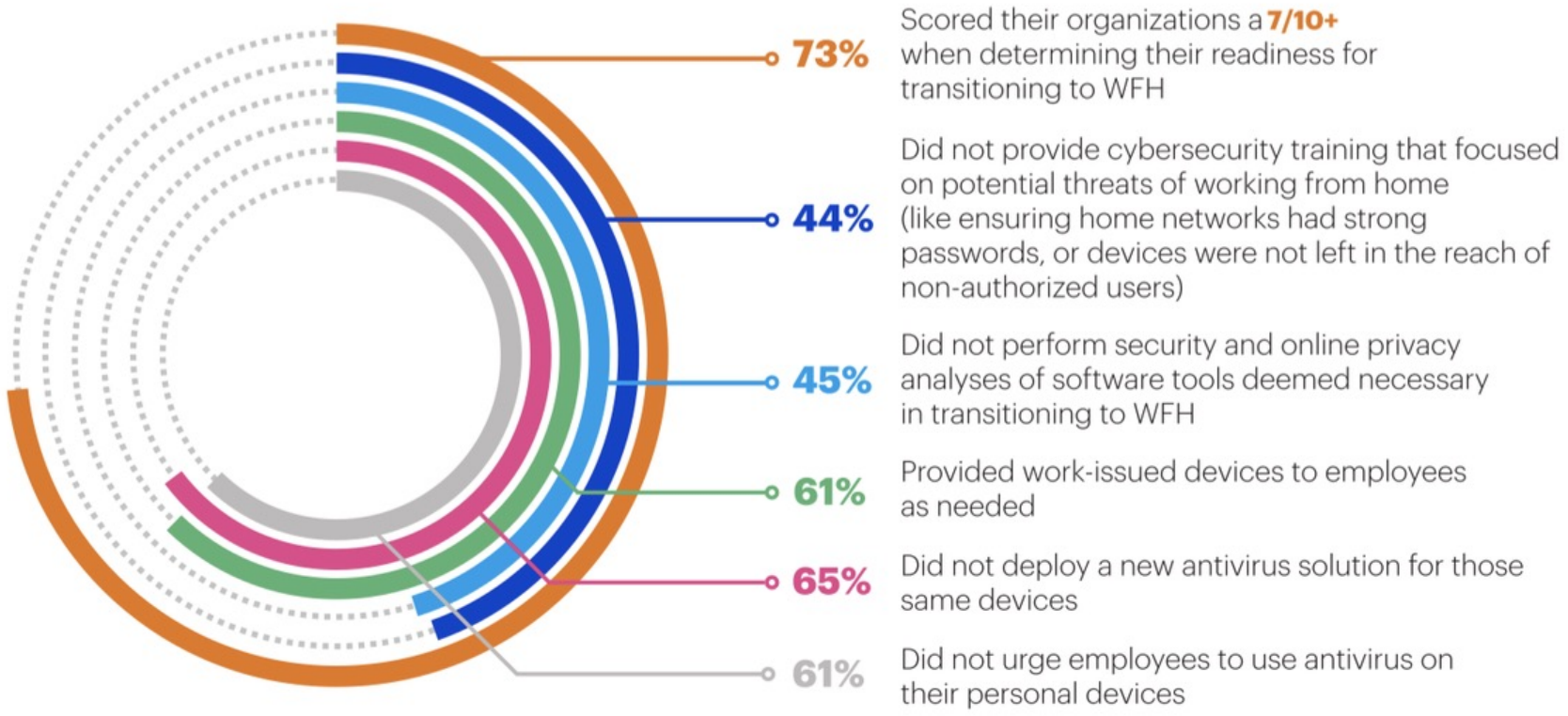
Frequency	Small (less than 1,000 employees)	Large (more than 1,000 employees)
	407 incidents, 221 with confirmed data disclosure	8,666 incidents, 576 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 70% of breaches.	Everything Else, Crimeware and Privilege Misuse represent 70% of breaches.
Threat Actors	External (74%), Internal (26%), Partner (1%), Multiple (1%) (breaches)	External (79%), Internal (21%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (83%), Espionage (8%), Fun (3%), Grudge (3%) (breaches)	Financial (79%), Espionage (14%), Fun (2%), Grudge (2%) (breaches)
Data Compromised	Credentials (52%), Personal (30%), Other (20%), Internal (14%), Medical (14%) (breaches)	Credentials (64%), Other (26%), Personal (19%), Internal (12%) (breaches)

Source: 2020 Verizon Data Breach Investigations Report (DBIR).

- 86% of breaches driven by financial gain (+ 15% vs 2019)
- 70% of breaches are caused by bad actors
- 67% of breaches were due to credential theft, errors and social attacks
  - 37% of credential theft breaches use stolen or weak credentials
  - 25% involve phishing
  - 16% from password dumps
  - Human error accounts for 22% of breaches
- 27% of malware incidents are from ransomware, which are growing
- 43% of breaches are due to web app attacks (2x 2019)
- 58% of breaches involve personal data (2x 2019)
- 17% of breaches are caused by errors (2x 2019)
- 43% of data attacks are cloud-based (2x2019)
- 20% of attacks are against web applications using stolen credentials

03 Impact of COVID & Telework

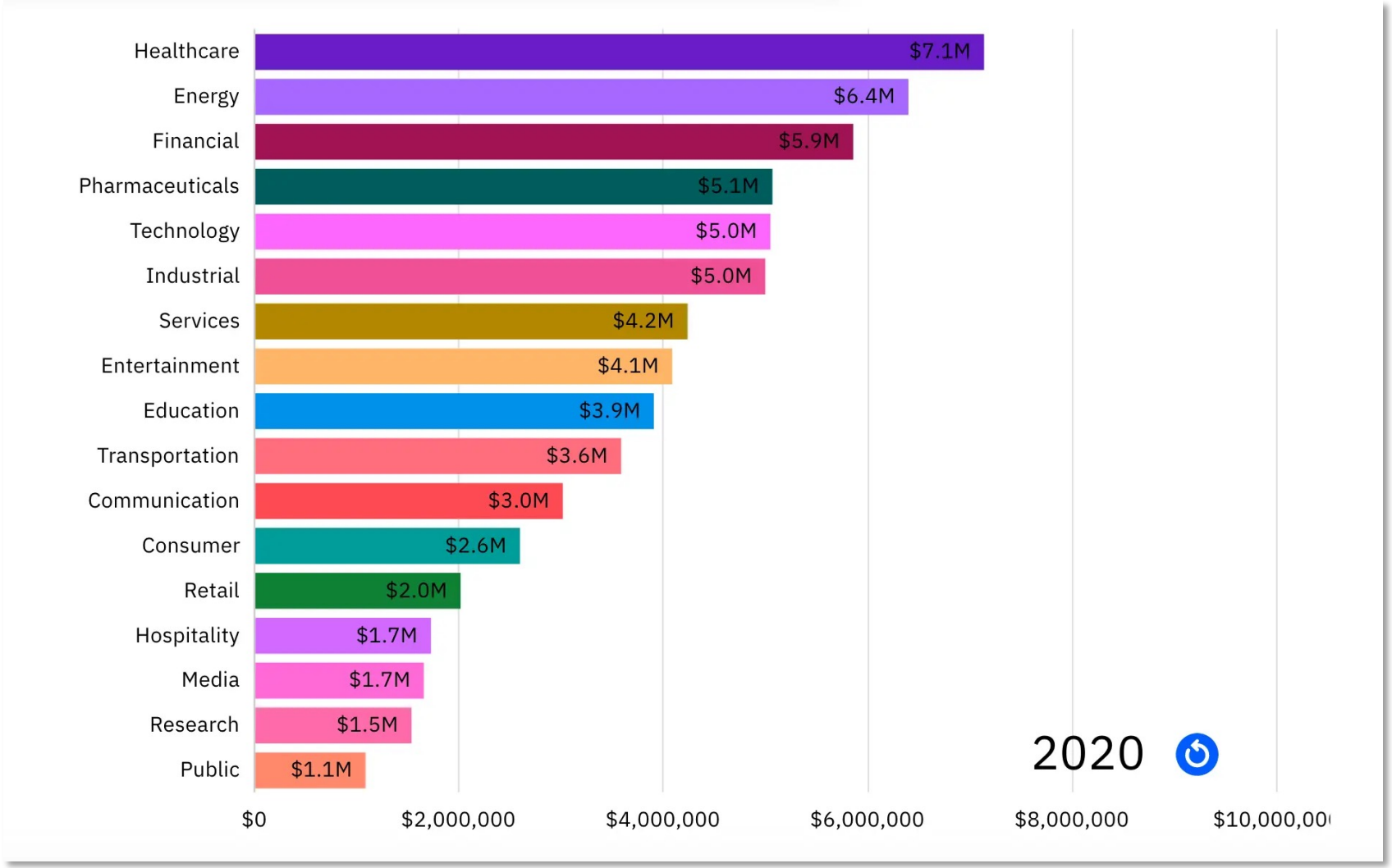
RISK



- COVID-19 and the rushed response to shift to virtual operations further compounded vulnerabilities in cybersecurity plans.
- 45% of organizations did not implement additional security checks or audits to safeguard work from home changes.
- 61% of organizations did provide their staff with secure remote working devices.
- 65% did deploy new or additional security tools together with the equipment.
- One in Five SMBs do not use any Endpoint Security Protections.

03 Average Breach Cost

RISK



Source: Ponemon Institute, Cost of a Data Breach 2020

03 Average Breach Cost

RISK

Detection and Escalation Costs

- Forensic and investigative activities.
- Assessment and audit services.
- Crisis management.
  - Notifications
  - Public Relations
  - Legal/Litigation
  - Compliance
- Communications to executive management and board of directors.

Hidden Costs

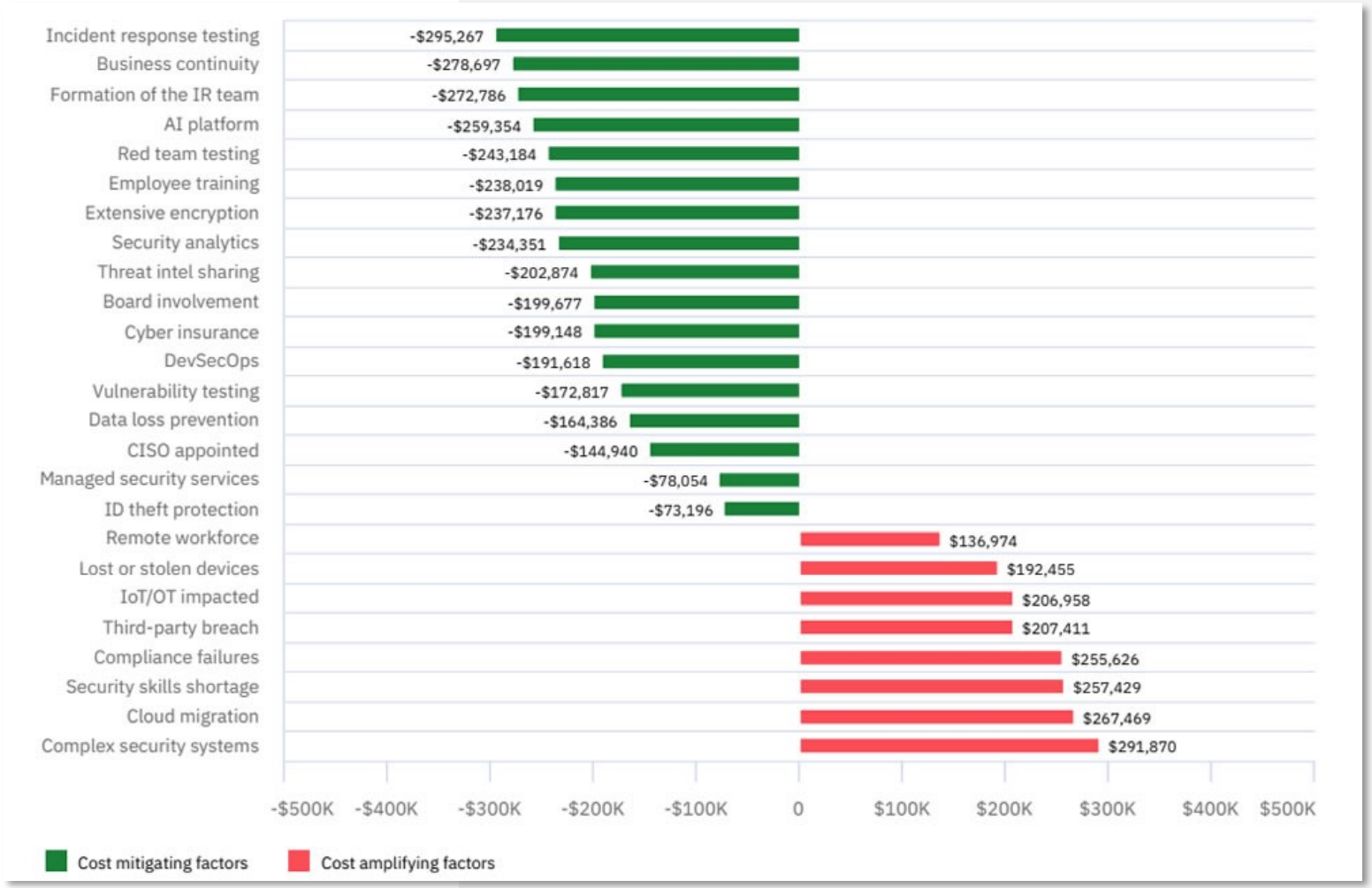
- Insurance premium increases.
- Increased cost to raise debt.
- Operational disruption or destruction.
- Lost value of customer relationships.
- Value of lost contract revenue.
- Devaluation of trade name.
- Loss of intellectual property.
- Reputational risk.
- Stock price volatility.

03

RISK

Key Factors Affecting the Cost of a Data Breach

- Organizations in the United States faced the highest data breach costs, with a typical breach costing $3.86 million, up 5.5% from 2019.
- Mitigation factors helped reduce total cost of breaches and downtime.
- Incident response plans and testing has proven to reduce total breach costs most.
- Employee training also has a significant impact on breach costs.
- Leading cost amplifiers include third party vendor breaches, remote work force, and cloud migration.

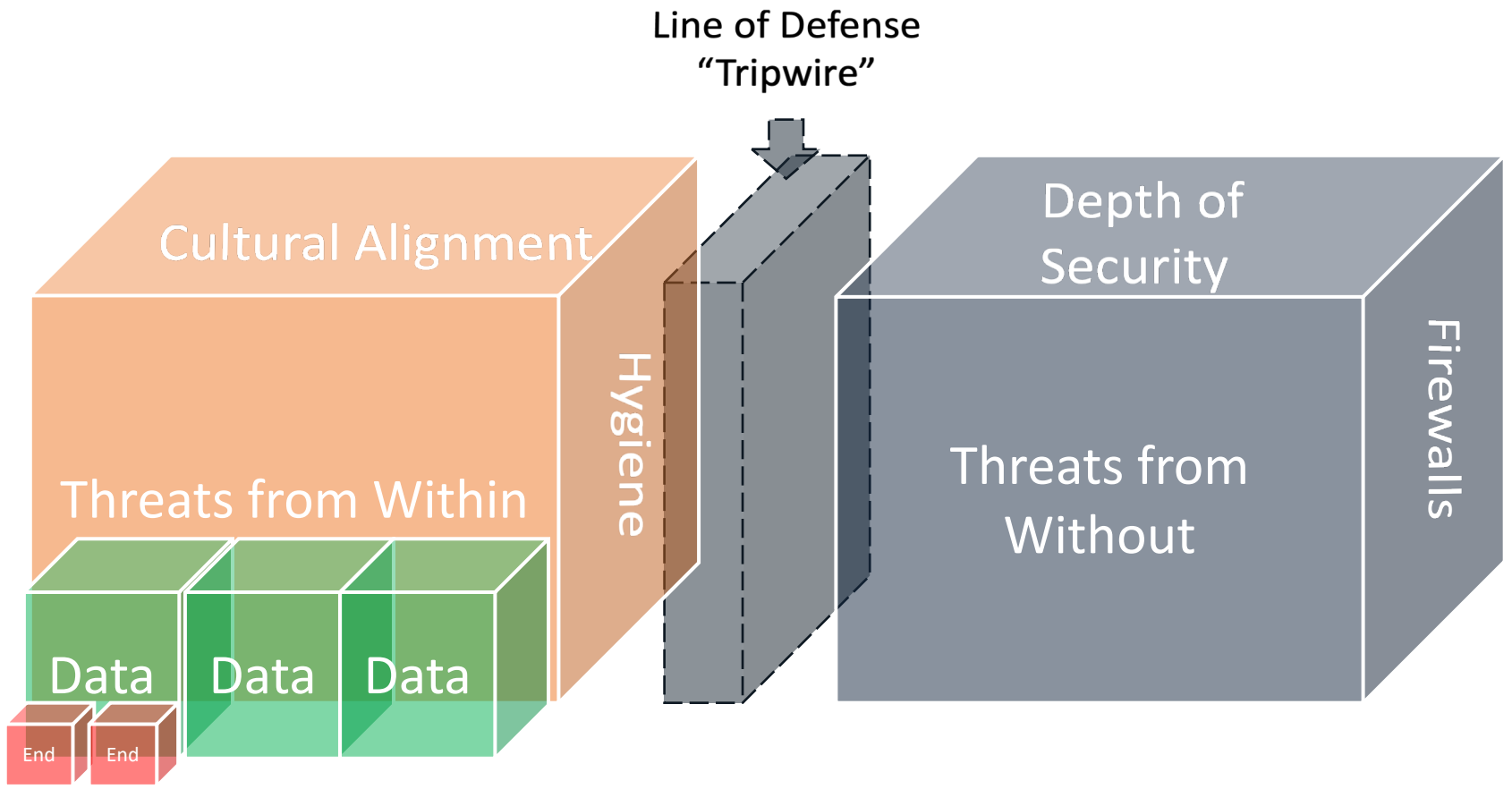


Source: IBM Security: 2020 Cost of a Data Breach Report

04 Cyber Risk & Security Matrix

STRATEGIES

- The amount of money spent on security or technology solutions is not a proxy for cyber-security.
- Organizations with robust cybersecurity culture, and top-down enforcement of these policies are best suited to withstand and prevent attacks.
- The biggest cyber risk and the most effective cybersecurity resource often lies between the chair and the keyboard.



04 Building a Governance Framework

STRATEGIES

A RESILIENT ORGANIZATION CANNOT RELY ON ONE SINGULAR COMPONENT.

People

Do you have a culture of proactive cybersecurity?

Are roles, responsibilities and priorities defined?

Does your organization chart and accountabilities reflect the importance of cybersecurity to your enterprise?

Processes

Do you have cybersecurity policies in place?

Do your onboarding/termination procedures include cyber elements?

Do you have established procedures for allowing access to your networks and infrastructure?

Do you have plans and procedures for emergency response and business continuity?

Do you have cybersecurity insurance? Do you understand its requirements?

Technology

Do you utilize firewalls as well as anti-virus and anti-malware software?

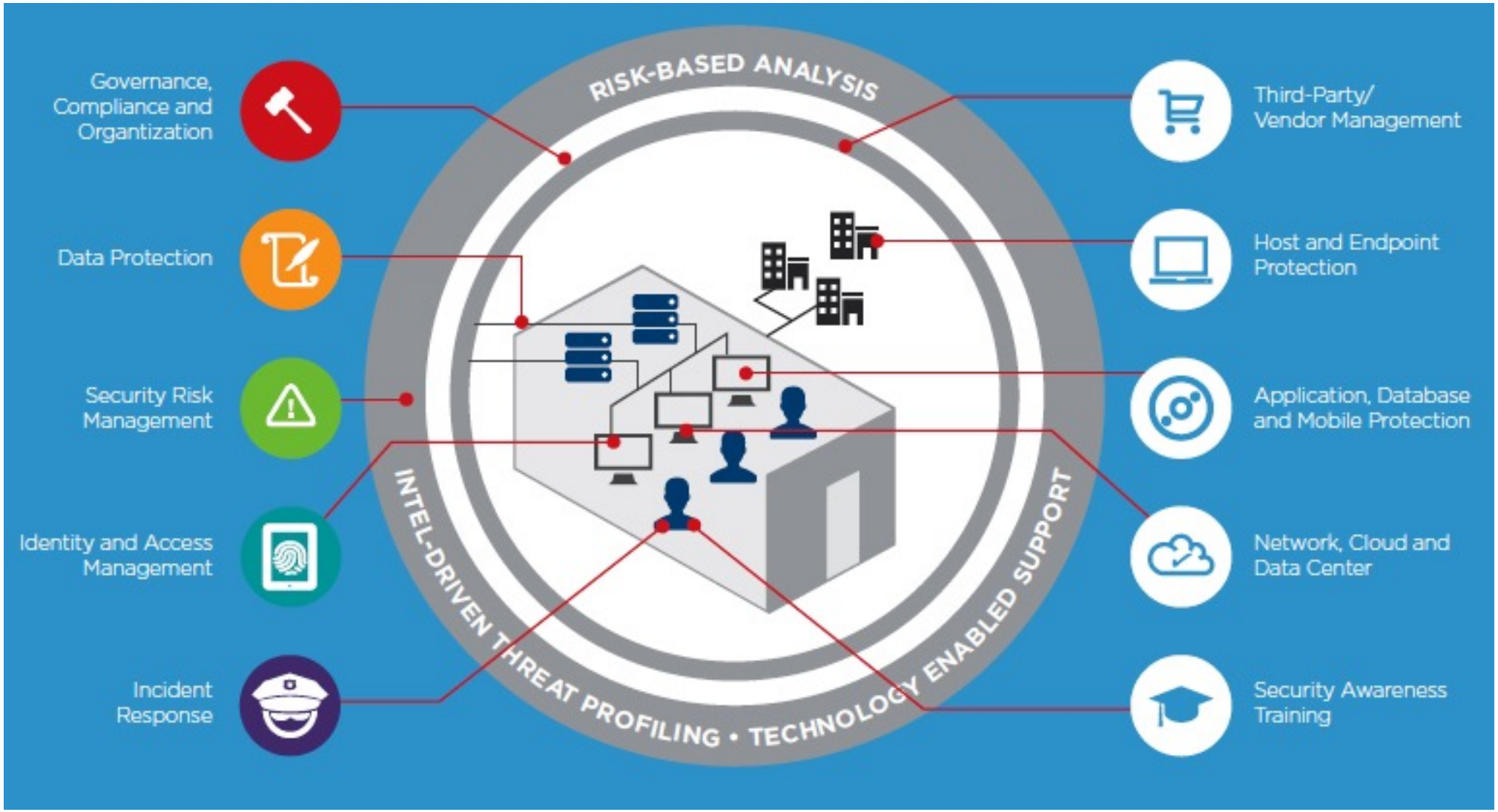
Are these technologies kept up to date?

What monitoring capabilities do you employ?

Do you encrypt data?

Do you have “tripwires” in place guarding against exfiltration?

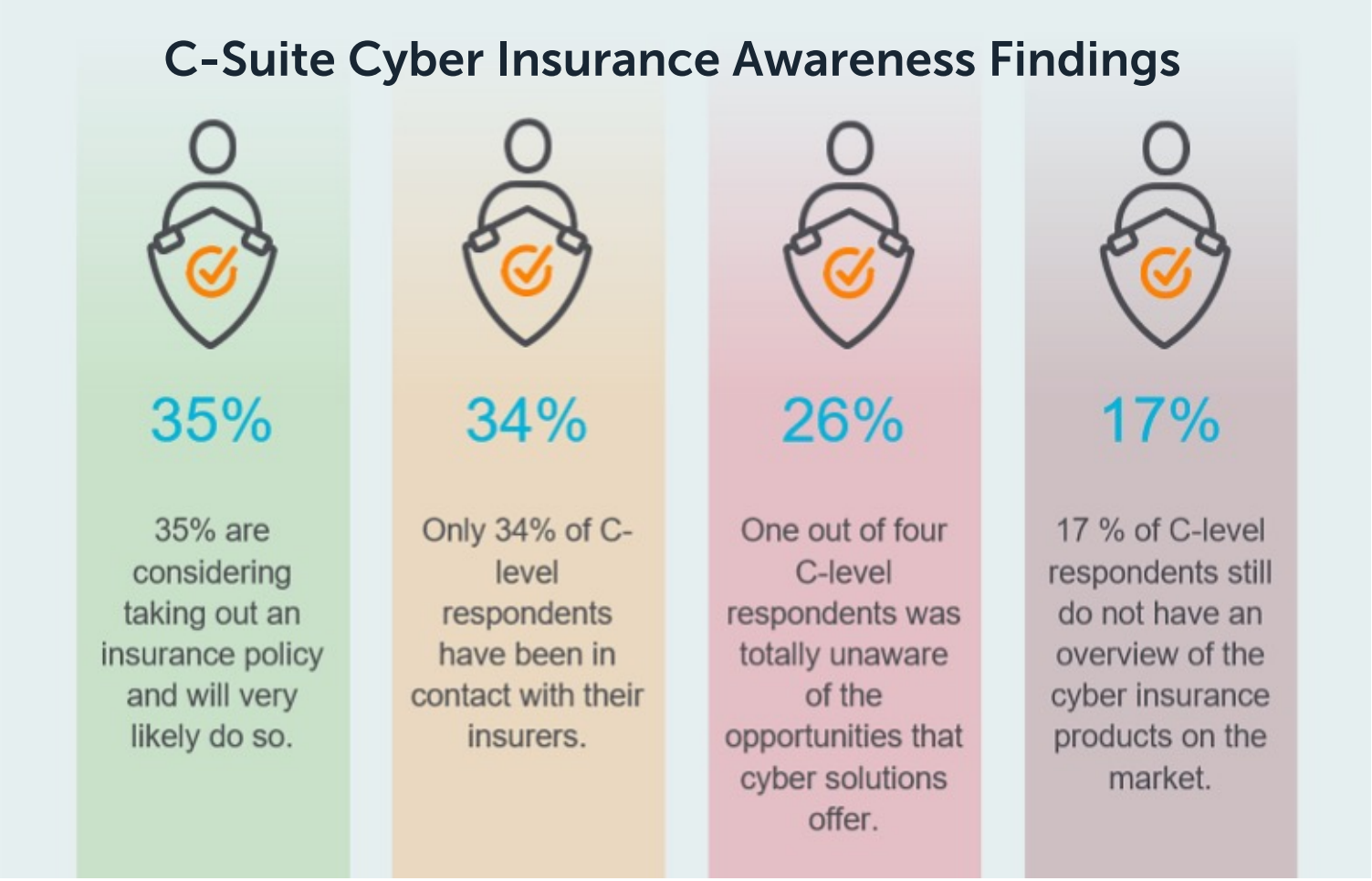
04 Critical Cyber Security Components



04 Additional Mitigation | Cyber Insurance

STRATEGIES

- Another key mitigation tool is cyber insurance.
- Companies can use cyber insurance as a financial hedge to limit the potential liability and economic damage incurred as a result of a cyber attack.
- Yet, the cyber insurance landscape remains mysterious and aloof to many organizations.
- Recent surveys showed the majority of C-level executives, while concerned about cyber threats, are largely unaware of the cyber insurance products and services available on the market.



Covered Cyber Losses

The the proper type of cyber insurance can reduce the risk of interruption and losses for companies and the supply chains they comprise.

Shapes

- First Party Loss
- Third Party Loss

Color Key

- Covered by a traditional cyber policy
- Covered by a traditional cyber policy and possibly by a robust errors & omissions policy
- Covered by a cyber policy and possibly by a property policy
- Covered by a specialized traditional cyber policy and possibly by a property policy
- Potentially covered by an enhanced cyber policy
- Potentially covered by an enhanced crime policy and by an enhanced cyber policy
- Covered by a traditional cyber policy and potentially by a kidnap and ransom policy
- Potentially covered under specialized cyber policy and under property and casualty program
- Uninsurable under current market conditions

04 Not All Cyber Policies Are Created Equal

STRATEGIES

- Bundled products are the source of systemic risk in the insurance balance sheet.
- Courtrooms increasingly determining claims outcomes.
- Cyber insurance brings breach panel and outside resources most companies do not have in house.
- You can't buy insurance when the house is on fire.

Bundled

- Bundled programs
- Directors and officers
- General liability
- Property insurance
- Errors and omissions

EDP

- Data processing equipment
- Hardware replacement
- Property coverage

Danger Zone

Stand-Alone

- Third party liability
- Breach Response
- Notification
- Restoration
- Business interruption
- Reputation risk

Stop-Loss (DIC)

- Catastrophic backstop
- Covers gaps
- Meant for large Losses above first layer cover.

Depleted Underlying Coverage

Safe(r) Zone

Cyber Insurance Market Trends

A recent report from Allianz insurance provided key cyber insurance and claims trends. Key findings included:

- Business interruption (BI) losses accounted for 60% of cyber insurance claims in the past five years.
- Analysis of more than 1,700 cyber insurance claims worth $793m in the past five years also reveals that the average cost of cybercrime for organizations has increased 70%.
- There were 770 claims lodged with AGCS in the first nine months of 2020.
- This follows 809 for the whole of 2019.
- Almost half a million ransomware incidents were reported globally last year, costing at least $6.3bn in ransom demands.
- Total costs are thought to be in excess of $100bn.

04

STRATEGIES

8 Key Mitigation Measures

Cyber is a complex risk that continues to evolve. Unlike other risk categories, it has agency and can adapt to defenses. In order to combat cyber risk and mitigate potential attacks, some first steps can include:

01 Clear Policies & Protocols

A key and basic first step that organizations of all sizes should take, is to ensure there are clear cybersecurity policies and protocols in place. Equally important is that these policies are actively enforced and tested on a regular basis.

02 Access Management

Access management is another basic measure that organizations should take to protect their control systems. Identity Access Management (IAM) in databases and other important IT infrastructure is necessary to limit access and prevent the misuse or leak of information. Personal and work resources to be separated, with sensitive company information not to be stored on any personal devices or shared publicly through social media. Using an authentication process for verifying instructions like wire transfers. Rules regarding the opening of links or attachments to be clearly stipulated.

03 Awareness as Defense

One very effective way of preventing cyber attacks on an enterprise is to train the employees in the basics of cyber security. Cyber aware employees form a major defense against attempted cyber attacks on the enterprise.

04
STRATEGIES

Eight Key Mitigation Measures

04 Email Domain Security

To ensure the security of an organization, it is imperative to address the cyber threats originating from its email domain. Using email domain security tools can be very effective in stopping spoofing of the email domain to protect the enterprise against spear-phishing attacks. Additionally, all emails which include private information such as bank details, credit card numbers etc. to be encrypted.

05 Data Backup

Frequent data backup in offline locations in a segmented manner is the best approach to defend against ransomware attacks.

06 Incident Response

Develop a clear and concise cyber incident response plan that is communicated to all staff. Use of incident response tools can further facilitate quick detection of and response to a cyber attack. A phishing incident response tool can be helpful in identifying and removing phishing emails from the employees' inboxes.

07 Strong Passwords

Employees should be encouraged to use strong passwords. This applies to both their work emails and other credentials used for accessing information and operations of critical systems in the enterprise.

08 Risk Insurance

Cyber insurance can be another powerful tool to limit potential damage incurred by a cyber attack. Policies provide financial liability and income protection, as well as embedded breach response resources to help mitigate and contain a breach before bringing the organization back online after an intrusion event.

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

MAY 12 | 9AM

Your Strategy
for Cyber Recovery

Please join us again next week for Part 2.

Questions?

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