BCG

Executive Perspectives

# The CEO’s Guide to Cybersecurity

*September 2021*

# BCG Executive Perspectives

## IN THIS DOCUMENT

## CYBERSECURITY HAS BECOME INCREASINGLY PRESSING

Even prior to the COVID-19 pandemic, the global cost of cyber crime had been surging. The frequency and severity of cyber attacks continues to accelerate as cost per attack decreases and defense requirements rise. During the pandemic, the cyber attack surface has further expanded. Due to a large increase in the number of people working from home and a spike in digital adoption broadly, there has been a rise in unsecured technologies (e.g., networks, devices, platforms) and accompanying processes. Attackers have seized the chance to exploit new vulnerabilities in unprepared workforces.

## CEOS CAN SPEARHEAD CYBERSECURITY STEP CHANGE

Cybersecurity is often viewed as an intimidating topic and a purely technical issue. But it is not only up to the IT department or the chief information security officer (CISO) to defend against malicious actors. CEOs, boards, and the C-suite need to strengthen cybersecurity programs and integrate them into broader strategies. They must ask challenging questions, hold leaders accountable, and ensure everyone is trained on appropriate protocols. A well-functioning cyber program not only helps protect crown jewels but can also be a strategic differentiator.

Sources: BCG analysis and case experience.

# Cybersecurity has become an increasingly pressing issue of greater scale

## Rising costs

**~$2T**

Estimated cost of **cyber crime** by end of 2021, up from **~$400B** in 2015

## Increasing impact

**$265B**

Estimated global cost of **ransomware damage** in 2031, up from $20B in 2021 as attacks increase in **frequency** and **severity**, which can affect operations

## Human error

**77%**

Of cyber attacks are due to **human** and **not technological failures**

## Protection gaps

**84%**

Of companies do not effectively mitigate **third-party cyber risks**

## Quantum future

**5-10**

Years before **quantum computing** potentially becomes **commercially available**, overturning today's encryption standards

Sources: BCG *Ensuring Online Security in a Quantum Future* (March 2021), Worldometer, CNBC, World Economic Forum, Cybersecurity Ventures, Ponemon Institute, press search, BCG analysis of 50 major data breaches (2021), BCG analysis.

# As COVID-19 expedites digital connections and increases cyber risks, the breadth of impacts from cyber attacks also expands

Examples of potential wide-reaching cyber impacts

Illustrative

**Security**
Security systems could be deactivated

**Utilities**
Power, water, or gas services could be stopped

**Cellular & Wi-Fi**
Phone and internet connectivity could be compromised

**Health**
Hospital data and systems can be altered, placing lives at risk

**Retail**
Millions of customers' personal data could be compromised

Summary

# The CEO's Guide to Cybersecurity

1 **CYBERSECURITY TRENDS**

1 Global cost of cyber crime is rising precipitously, driven by lower cost to execute attacks and higher complexity to defend; public and private sectors struggle to respond

2 As pandemic drives massive increase in digital/devices, cyber attacks are rising even more

3 Most cyber attacks are due to human failures (e.g., people, processes) rather than technology

4 Cyber risks are beyond financial (e.g., operations) and can threaten an organization's existence and even human safety (e.g., attacks on infrastructure/machinery, health care)

5 As supply chains become more digital and complex, they are increasingly targeted for attacks

6 Quantum computing may be widespread in 5-10 years, leading to overhaul of cyber standards

2 **IMPLICATIONS FOR LEADERS**

Critical for CEOs to set cyber ambition and integrate cybersecurity into business processes/strategy

1 Orient organization's cyber ambition relative to industry peers and investment ability

2 Rethink prevention and detection of near-term attacks; build cyber into business strategy

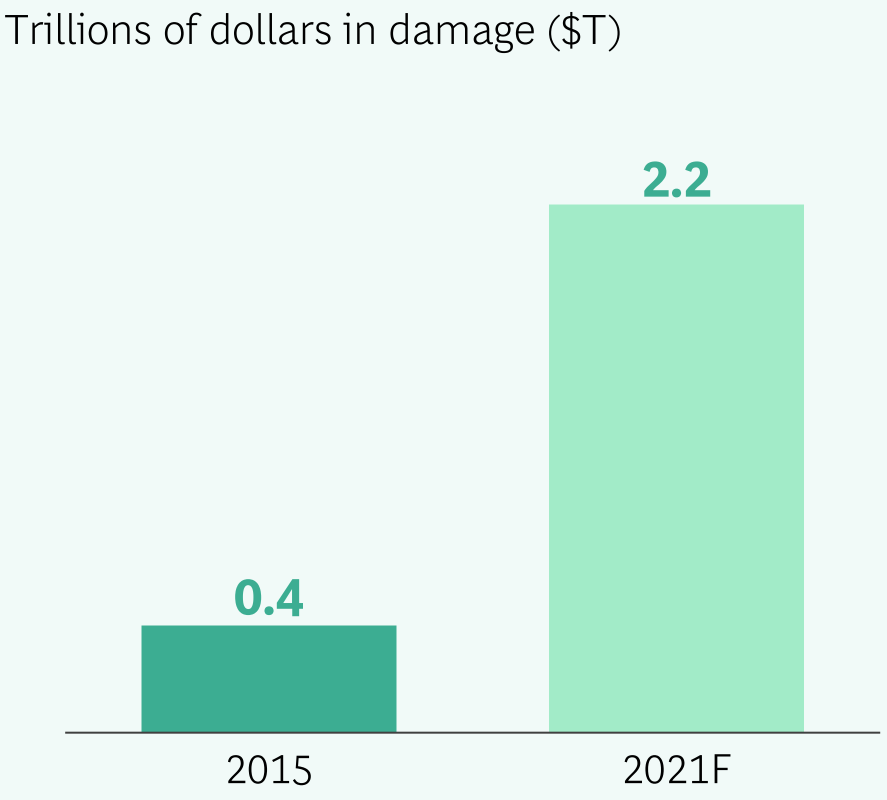
3 After a breach, leaders must collaborate to notify third parties, investigate, and communicate

4 Future-proof cybersecurity by considering increased risk from emerging/new technologies and behavior changes

Sources: BCG analysis and case experience.

# 1.1 A Global cost of cyber crime is projected to rise from $445B in 2015 to $2.2T by the end of 2021, marking a ~5X increase

## Global cost of cyber crime has risen rapidly with sophistication and scale



Sources: Cybersecurity Ventures, World Economic Forum, press search, BCG analysis.

## Public and private sectors battle impacts from hacks, such as lawsuits and sanctions

**$20B** Estimated cost of global ransomware damages in 2021

In 2021 alone, there have been major cybersecurity breaches, leading to **hundreds of millions** of stolen data records. For example, a software-firm hack in February led to data compromises across 9 federal agencies and 18K companies

Prominent hacks this year led to the issuance of the **US Cyber Executive Order** in May, which established new rules for government suppliers for enhanced cybersecurity

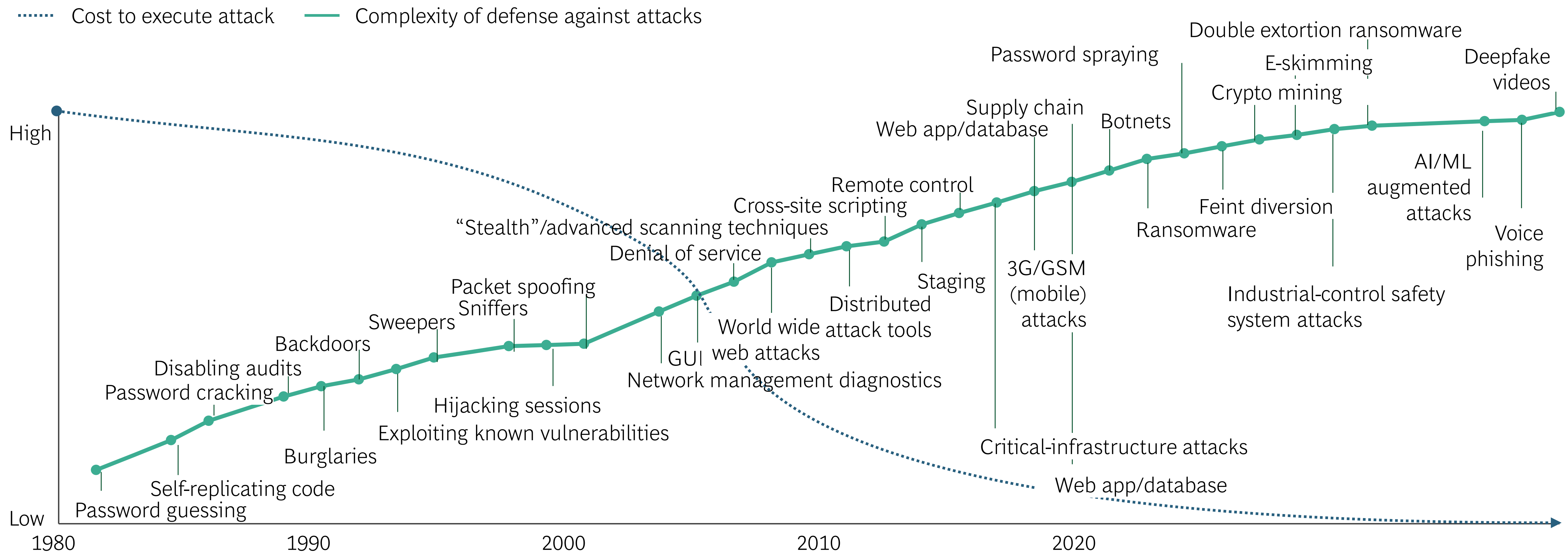
Private companies wrestle with the impacts as they are hit with **class-action lawsuits** from employees, customers, and partners after ransomware attacks (e.g., after pipeline hack, customers sue as supply dried up) and increasing **regulatory fines and sanctions**

1.1
B

# As cost to attack decreases, required complexity of defense increases

## Cyber attacks are increasingly cheaper to execute as technology advances; this leads to a need for increased complexity of defense

Illustrative



Sources: BCG *Navigating Rising Cyber Risks in Transportation and Logistics* (August 2021).

# 1.2 As pandemic drives a massive increase in digital and devices, cyber attacks are rising even more as the attack surface expands

## There has been a large increase in cyber attacks during the pandemic…

**~600%**

Spike in phishing attacks in the first quarter of 2020

**~80%**

Of IT teams saw a rise in cyber attacks in 2020

**~50%**

Increase in health care system hackings in the US in 2020

Sources: Forrester, Infosecurity Magazine, BCG *How Health Care Providers Can Thwart Cyber Attacks* (2021), Sophos, KnowBe4, BCG analysis and case experience.

## …as COVID-19 greatly accelerated digital transformations and drove reliance on IT

During COVID-19, there was an increase in digital adoption and devices online, thus increasing the **attack surface** and creating more opportunities for attackers. These changes are likely **longer-term trends**

### Key drivers of digital adoption:

There was rapid growth in **digital platforms and cloud adoption,** such as online commerce and digital tools. While the technology is likely more secure, there may be gaps in processes/training, leading to vulnerabilities

Employees **working from home** were connecting remotely over unsecured networks, on personal devices, etc.

Disruption in existing business practices created **operational instability** and led to vulnerabilities

1.3

# 77% of cyber attacks are due to human failures (e.g., people, processes) rather than technology

## Only a quarter of cyber breaches are caused by technology issues…

**Typical focus of attention**
(and important)

Inadequate technology causes **23%** of breaches …

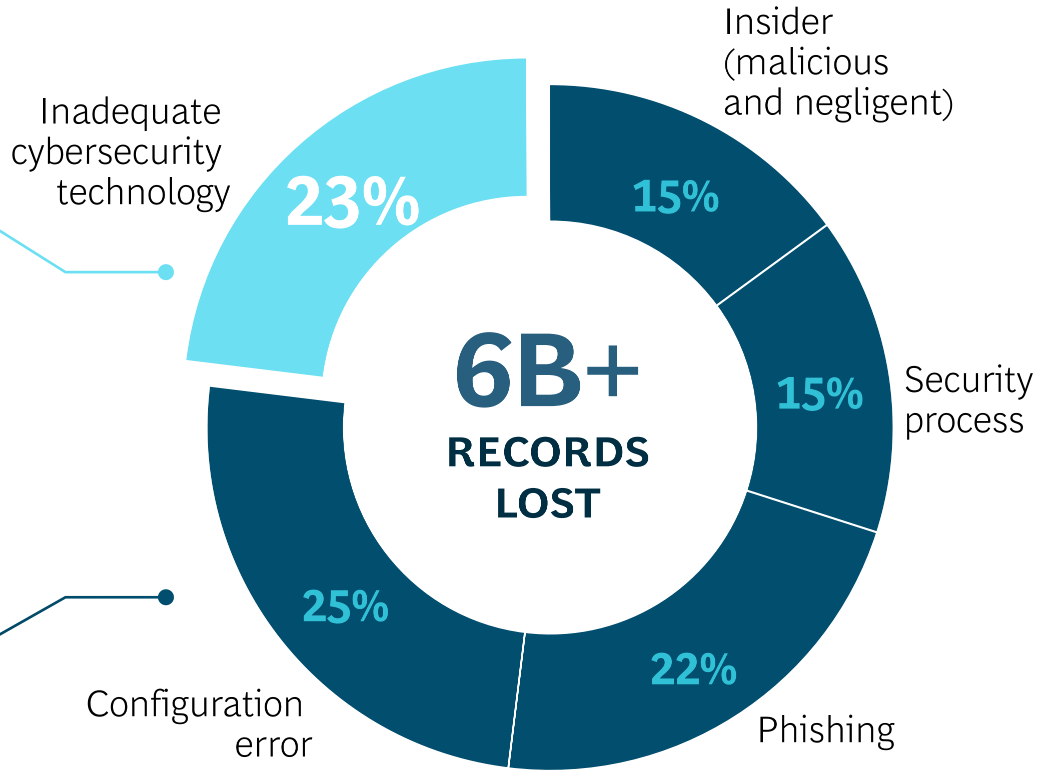
**Often neglected**
(but at least equally important)

… organizational, process, and people failures cause **77%**

Sources: BCG analysis of 50 major data breaches (2021).

## …whereas the remaining three-quarters are caused by human failures such as negligence or phishing

**Reasons for cyber breaches**



# 1.4 Cyber risks extend beyond direct financial impacts and can create existential company risk or human safety issues if not managed

## Cybersecurity is a top priority for boards, CEOs, and C-suites across regions[1]
## Failing to manage cyber risk may lead to financial and other consequences

### Direct financial risk

Cyber criminal used forged invoices to steal over **$100M** from large tech companies

Other direct financial risks include **ransoms, class-action lawsuit payouts, and share price impacts**

For example, a financial services vendor lost **$8B** in value after hackers stole data on **100M+** customers

### Catastrophic risk

Enterprise software company put out of business as attacker **deletes all data and backups**

### Reputational risk

Telecom company lost over **100K customers and 1/3 of company value** after breach

### Regulatory risk

Regulators punished transportation company with **$148M fine for failing to report** data breach

### Operational risk

Bank data-theft attack **disrupted operations** for 2 weeks after wiping computers to hide fraud

### Strategic risk

Stolen R&D data from drug manufacturer led to fast competition with **counterfeits**

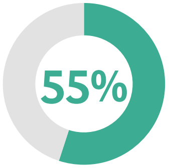
### Health and safety risk

Hackers took control of furnace at steel mill, **preventing safe shut-down** and causing massive damages

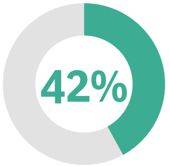
Note: These are sanitized descriptions of actual attacks. 1. Cybersecurity attacks are the top business threat in North America, #2 in Europe, and #5 in Asia-Pacific.
Sources: World Economic Forum *Top Perceived Risks of Doing Business* (2020), BCG analysis, press search.

# 1.5 As supply chains become more digital and complex, they are increasingly targeted for attacks

## Attackers are increasingly exploiting supply chain vulnerabilities…



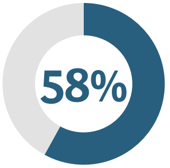
Of attacks happen through **supply chains** instead of directly targeting the company, as unprepared suppliers can be a **weak link**



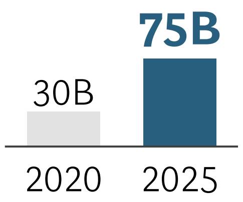
Increase in **supply chain cyber attacks** in the first quarter of 2021

In addition to direct attacks, attackers are increasingly engaging in a method called "**island hopping**," in which they also aim to affect the victim's **partners and customers**

## …as there are more opportunities to attack in connected and complex supply chains



Of workloads will be hosted in **public and private clouds** by 2023. While cloud technology is safer, **improperly managed processes** can create risk



Connected **Internet of Things** (IoT) devices by 2025. Many newer devices **do not have enough** cyber protections built in or considered in design

**Increased reliance** on suppliers leads to reduced **transparency of risk**. There is also a need to secure an exponentially increasing number of **endpoints** as **connected devices** proliferate

Supply chains are one of the **most difficult** areas to secure because of the **lack of visibility and full control**
More companies and regulators are becoming aware of this growing gap and are continuing to look for viable solutions

Sources: Ponemon Institute, Carbon Black, Identity Theft Resource Center (ITRC), Sonatype, BlueVoyant, Fortune, TechRepublic, press search.

# 1.6 Quantum computing may become widespread in as little as 5-10 years, creating a need to overhaul encryption standards

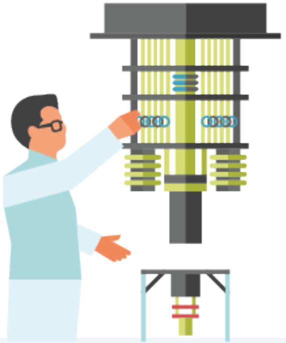
## Why it matters | Once commercially viable, quantum will render existing encryption standards obsolete. Even if action is not immediately required, leaders can think ahead

1 | Existing or classical computers use **bits** to store information

2 | Classical computers utilize encryption standards based on finding **prime factors** of large numbers hundreds of digits long

3 | Quantum computers use more powerful **qubits**, enabling exponentially greater computational **speed** (up to **100T times** faster[1])

Once algorithms are developed, they would be able to **hack** into today's secure systems



4 | Quantum computers, once thought to be science fiction, are now **on the horizon (5-10 years)**.[2] They may not fully replace classical computers but will be much better at certain jobs

5 | Currently, quantum computers do not have wide practical use cases. If **commercially viable**, however, they would **revolutionize** the world

While there will be major advances, today's encryption standards would be **obsolete**, leading to a **new race** between attackers and the vulnerable

[1] A team in China developed a quantum computer that performed a calculation in 200 seconds that would take a classical computer 2.5B years – an improvement of 100 trillion times.

[2] Google is aiming to build a viable quantum computer by 2029. Sources: BCG *Ensuring Online Security in a Quantum Future* (2021), press search.

# Cyber attacks continue to generate headlines as new technologies make it possible to create increasingly larger impacts

**As of 26 August 2021**

August 26, 2021

Biden calls cybersecurity “core national security challenge” in meeting with tech, education, and infrastructure leaders

August 18, 2021

T-Mobile says hackers stole data on more than 40 million people

July 12, 2021

Microsoft to acquire cybersecurity firm RiskIQ after breaches to Microsoft Exchange servers

July 7. 2021

Up to 1,500 businesses could be affected by a cyberattack carried out against Kaseya

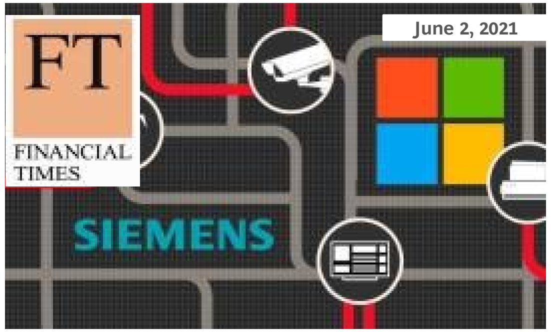
Bloomberg
Belarus hackers seek to overthrow government
Hackers release data of alleged police informants, government spies
Bloomberg Quicktake

August 24, 2021

Belarusian hackers seek to overthrow national government

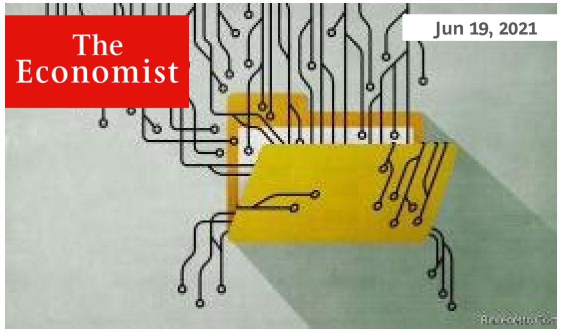
August 19, 2021

Hackers steal nearly $100M, in Japan crypto heist targeting Liquid



June 2, 2021

Millions of connected devices have cybersecurity flaws, study shows



Jun 19, 2021

Ransomware highlights the challenges and subtleties of cybersecurity

# 2 It is critical for CEOs to set the cyber ambition and integrate cybersecurity into their business processes and broader strategy

Cyber transformation plan

## 4 actions for CEOs to build cyber capabilities

### STEP 1

Determine need and ability to **set cyber ambition** for silver or gold levels – align with business strategy

| | Cyber response |
|---|---|
| Bronze | Reactive |
| Silver | Proactive |
| Gold | Anticipatory |

### STEP 2

Increase preparedness by understanding own maturity and focusing on **tangible wins,** then **scaling** cyber program across organization

### STEP 3

In the event of a breach, avoid finger pointing; stay **aligned** across functions and ensure **transparency** internally and to third parties

### STEP 4

Watch emerging/new technologies to **avoid blind spots** and prioritize preparation for cyber **future**

Sources: BCG case experience, BCG analysis.

# Step 1 | Orient cyber ambition relative to industry, peers, and investment ability

## Most companies are at a bronze level of cyber capabilities today but should set ambitions to silver or gold as the dynamic threat landscape continues to evolve

Cyber ambition scale

| AMBITION | PROTECTION SCOPE | TECHNICAL PROTECTION | RESPONSE |
|---|---|---|---|
| Bronze<br>% of IT spend[1]<br>~5% | Focus on **crown jewels** protection only; senior management commitment and basic employee trainings | **Baseline** technical protection (e.g., anti-virus software, defined policies/procedures) | **Dispersed and reactive** detection and response |
| Silver<br>~10% | Risk-driven prioritization integrated into **business processes**; senior management **ownership** and advanced employee trainings | **Proactive** technical protection (e.g., code scans, security testing, multifactor authentication) | Centralized **incident detection and response** (especially via Security Operations Center and threat intelligence feeds) |
| Gold<br>~15% | Cyber risk management integrated **across enterprise** and corporate risk framework | Latest technical protection (e.g., **AI-based and highly automated**) | Anticipate and **preempt incidents** through automated cyber monitoring and pattern recognition |

[1] These levels are approximate. Investment requirements within ambition will vary significantly depending on industry, business complexity, region, and level of previous investment

Sources: BCG analysis and case experience.

### Transformation

Most cyber transformations will take at least **3-4 years** to complete. Companies should prepare to invest **upfront 5-6x** their annual cyber spending

### Industry context

Most sector leaders should **strive for silver** level ambition, but some sectors (e.g., finance, infrastructure, and telecommunications) require **gold level ambitions to be leaders**

2.2

# Step 2 | Rethink prevention and detection of near-term attacks and build cyber into business strategy

Near-term wins for cybersecurity programs

## Cyber attacks are inevitable, but preparedness can drive better outcomes

**4 areas for companies to take action to bolster cybersecurity programs:**

### PREVENT

Identify critical "**crown jewels**" and prioritize securing assets **based on their value** (cannot protect all). Benchmark overall maturity and spending to competitors

### DETECT

Invest in **robust monitoring** capabilities; best-in-class organizations detect breaches in minutes vs. weeks by focusing on **malicious activity and indicators**

### RESPOND

Run tabletop exercises (TTX) to ensure that management and employees are **prepared for roles and responsibilities** in event of a breach

### RECOVER

Build a cybersecurity culture where the focus is not on blame, but on **continuous learning and improvement**

Scale across company

### DESIGN CYBER INTO SYSTEMS

Integrate cybersecurity strategy into the broader **business strategy including development of processes** (for traditional and remote working models). Do not wait to add cyber at the end

### INCLUDE GOVERNANCE MODEL

Ensure that cybersecurity is top of mind **across the company** by building it into **governance** for organization and supply chain. Focus on **simplicity and scalability**

Sources: Ponemon Institute, Osterman Research, BCG case experience.

## Cyber as an enabler:

Strong cyber commitment not only prevents losses but can also be **a business enabler**

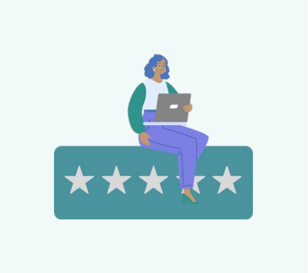
As consumers become increasingly concerned about the security of their information and the products they use, strong cybersecurity can be a **brand differentiator**—seen in industries like banking, insurance, and technology

2.3

Post-breach checklist

# Step 3 | If a breach occurs, top leaders must collaborate to notify key third parties, investigate, and communicate

## 10 steps for CEOs / CISOs / rest of C-suite to take following a breach:



### NOTIFY CRITICAL THIRD PARTIES

- ○ Inform cyber **insurance** carrier if any
- ○ Alert **banking and accounts payable** departments to scrutinize any large, anomalous transactions
- ○ Depending on the situation, consider contacting **law enforcement**
- ○ Ensure that regulatory-requirement actions for **personal identifiable information** (PII) are met in each region

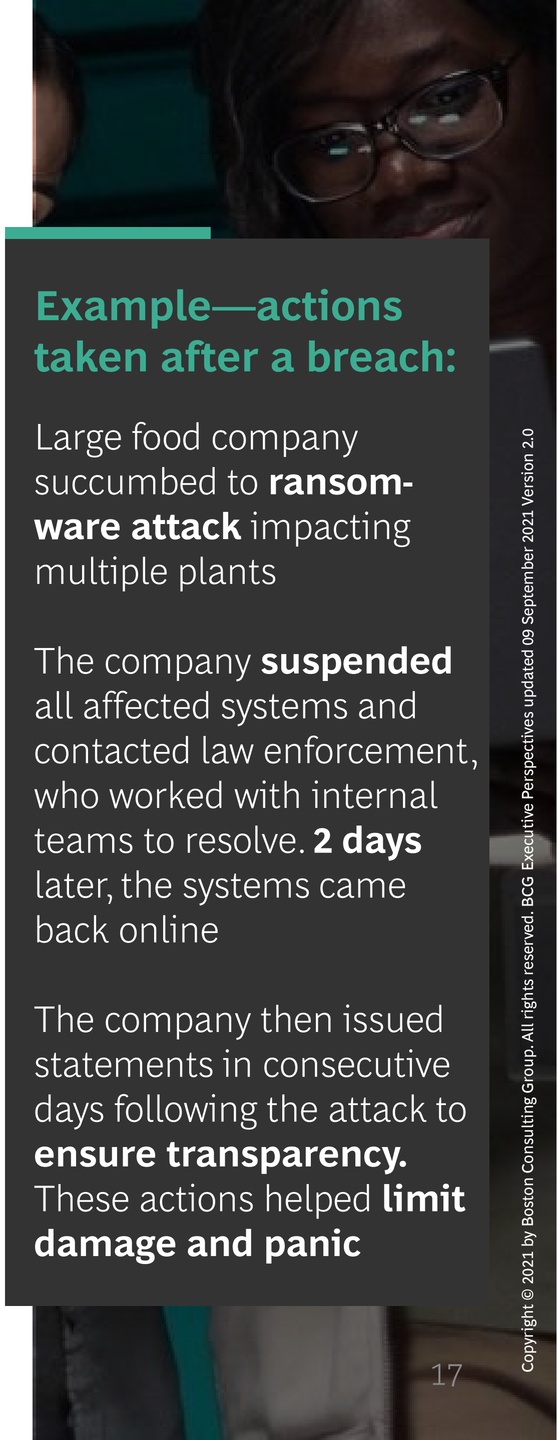
### INVESTIGATE INCIDENT

- ○ Investigate incident at all levels and collect as much **information** as possible, such as from employees. This could be used in a legal defense or lawsuit
- ○ Understand the **volume, type, and sensitivity** of the data exposed
- ○ **Decide** whether to allow the incident to continue in order to collect more data or stop the incident by terminating access and working with data already collected

### COMMUNICATE CLEARLY

- ○ Identify and confirm organizational **narrative** and cadence of **communications**
- ○ Communicate **internally and externally**, but do not make misleading statements. Be clear and direct with the information known at the time and state **action plan**
- ○ Convey that individuals should **not discuss** incident publicly and should **refer all inquiries** to central communications team

Sources: BCG analysis and case experience, press search.



## Example—actions taken after a breach:

Large food company succumbed to **ransomware attack** impacting multiple plants

The company **suspended** all affected systems and contacted law enforcement, who worked with internal teams to resolve. **2 days** later, the systems came back online

The company then issued statements in consecutive days following the attack to **ensure transparency.** These actions helped **limit damage and panic**

2.4

Long-term actions for lasting cybersecurity success

# Step 4 | Future-proof cyber by considering increased risk from emerging/new technologies and behavior changes

## Important to understand risks from emerging technologies to evolve cybersecurity programs accordingly

### 1 IoT/Ecosystem

Breadth of entry points is continuing to increase

Cybersecurity needs to keep up with **growth of internal devices** as well as risks posed from **outside supplier systems**

### 2 AI and automation

As AI continues to evolve, leverage this technology as a cybersecurity tool while **preventing AI attacks** from cyber attackers

Rise of automation will require **new monitoring** capabilities

### 3 Future computing

Cybersecurity safeguards must be revisited as **new computing technology resets paradigm** (e.g., plan for eventual quantum shift by inventorying all encryptions and identifying actions required)

### 4 Behavior changes

With hybrid work and potential changes to future talent models, it is critical to **invest in cyber education of employees and review business systems** to ensure a culture of cybersecurity, especially as people and processes make up a majority of breach entry points

## Example—Future-proofing:

Global retail group undergoing major digital transformation defined **cybersecurity strategy** to combat increased attacks

**Approach:** Conducted assessment, established risk map and crown jewels. Then developed plan with initiatives covering all key areas. Finally, derived longer-term future target state and model

**Result:** Discovered **50+** additional vulnerabilities and rationalized doubling the size of cybersecurity organization

Sources: BCG case experience.

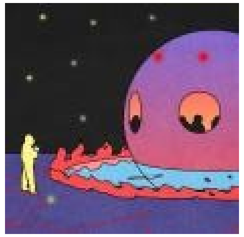
# Additional perspectives on cybersecurity

Managing the Cyber Risks of Remote Work

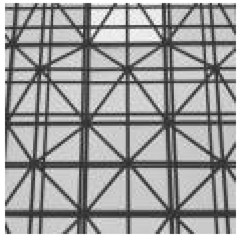
Five Ways Business Directors Can Prepare for the Future of Cybersecurity

Better Cybersecurity Starts with Honesty and Accountability

How Health Care Providers Can Thwart Cyber Attacks



Cyberattacks Are Inevitable. Is Your Company Prepared?



A Smarter Way to Quantify Cybersecurity Risk

Ensuring Online Security in a Quantum Future

Navigating Rising Cyber Risks in Transportation and Logistics

Are You Spending Enough on Cybersecurity?

Click here to read past editions of Executive Perspectives

Sources: BCG, HBR, Forbes, TED.

# Disclaimer

The services and materials provided by Boston Consulting Group (BCG) are subject to BCG's Standard Terms (a copy of which is available upon request) or such other agreement as may have been previously executed by BCG. BCG does not provide legal, accounting, or tax advice. The Client is responsible for obtaining independent advice concerning these matters. This advice may affect the guidance given by BCG. Further, BCG has made no undertaking to update these materials after the date hereof, notwithstanding that such information may become outdated or inaccurate.

The materials contained in this presentation are designed for the sole use by the board of directors or senior management of the Client and solely for the limited purposes described in the presentation. The materials shall not be copied or given to any person or entity other than the Client (“Third Party”) without the prior written consent of BCG. These materials serve only as the focus for discussion; they are incomplete without the accompanying oral commentary and may not be relied on as a stand-alone document. Further, Third Parties may not, and it is unreasonable for any Third Party to, rely on these materials for any purpose whatsoever. To the fullest extent permitted by law (and except to the extent otherwise agreed in a signed writing by BCG), BCG shall have no liability whatsoever to any Third Party, and any Third Party hereby waives any rights and claims it may have at any time against BCG with regard to the services, this presentation, or other materials, including the accuracy or completeness thereof. Receipt and review of this document shall be deemed agreement with and consideration for the foregoing.

BCG does not provide fairness opinions or valuations of market transactions, and these materials should not be relied on or construed as such. Further, the financial evaluations, projected market and financial information, and conclusions contained in these materials are based upon standard valuation methodologies, are not definitive forecasts, and are not guaranteed by BCG. BCG has used public and/or confidential data and assumptions provided to BCG by the Client. BCG has not independently verified the data and assumptions used in these analyses. Changes in the underlying data or operating assumptions will clearly impact the analyses and conclusions.