Deloitte.

What CEOs need to know about Cyber Security today

June 2022

In the digital age, cyber is everywhere. Which means cyber risk now permeates nearly every aspect of how we live and work.

Technology as the lifeblood

- Internet, cloud, social, mobile are mainstream -- platforms inherently oriented for sharing not security
- Attack surface is bigger, presenting more opportunities

Businesses built on cyber platforms

- Cyber technologies are now core to mission critical business services
- New businesses or business models are being created on cyber technologies
- Service models have evolved - outsourcing, offshoring, contracting, remote workforce

A mission to protect

- Various industry, & government regulations (especially privacy)
- Capital Markets' regulators focus on cybersecurity preparedness
- Protecting the economy & critical infrastructure
- Protecting shareholders

Threat actors with varying motives

- Hackers to nation states
- Continuously innovating & subverting common controls (e.g., anti-virus, user id/password)
- Often beyond the reach of country law enforcement

The convergence of forces is increasing the likelihood and impact of cyber risks.

Enterprise challenges in the new era

Exponential increase in attack surface

Legacy System & Technical Debt

Talent Shortages

Visibility Blind Spots & Inconsistent Execution

Cyber in Digital Transformation

Top threats currently facing the industry

Destructive Malware

Phishing

Credential Compromise

Supply Chain Attacks

Ransomware

Insider Threat

Business Email Compromise (BEC)

15 seconds Time required to break into a network using automated botnets [1]

58% Percentage of healthcare incidents involving **insiders** – Healthcare is the only industry in which **internal actors are the biggest threat to an organization** [4]

136% Percentage increase between December 2016 and May 2018 for identified global exposed losses due to BEC [7]

Ransomware variants have grown by more than 700% since 2016 [2] **700%**

14 seconds Businesses will experience ransomware attacks every 14 seconds in 2019 [3]

Ransomware attacks increased **threefold** in 2017, the ***Healthcare industry*** being the primary target [5]

Sources: [1] Cyber Reason https://www.cybereason.com/blog/botnets-honeypot-automation-cybersecurity [2] Gartner “Protect Your Organization From Cyber and Ransomware Attacks” February 14, 2018 [3] Cybersecurity Ventures “Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019” 14 November 2017 [4] Verizon 2018 Protected Health Information Data Breach Report [5] Cylance 2017 Threat Report [6] “2018 Data Breach Investigations Report”, Verizon [7] “Business E-Mail Compromise the 12 Billion Dollar Scam” FBI Internet Crime Compliant Center PSA Jul 12, 2018

Most common threat actors

Russia, Iran, China, N. Korea

- *Russian harbors a large proportion of the world's active cyber criminals*
- *The Iranian regime has conducted the most cyberattacks in peacetime than any other nation.*
- *People's Republic of China has engaged in espionage against government organizations globally for decades to accelerate their own developments*
- *North Korea has grown increasingly sophisticated in its ability to engage in increasingly hostile cyber activities*

Hactivists

Hacktivist attacks are often simplistic and often involve simple website defacements to cause embarrassment.

Although not the norm, there are cyber-activist groups that exhibit great technical skill and can make a significant global impact

Well-known hacktivist groups like WikiLeaks leak classified documents, private company information, sensitive data, and government information

Insider Threats

Employees are usually the most dangerous threat actor, knowingly and unknowingly.

Insider actors are usually current or past employees who can use their authorized access to gain company information.

Motivations are usually derived from discontent, revenge, or financial gain.

Many actors unknowingly go to malicious sites or click on malicious links.

Cyber Criminals

Cyber criminals are threat actors who steal sensitive information, financial records, person credentials, and bank account details via:

- *Ransomware,*
- *Phishing attacks,*
- *Malicious software*

These attackers are usually motivated by financial gain, and business data they obtain can often be found on the dark web or is sold to a third party

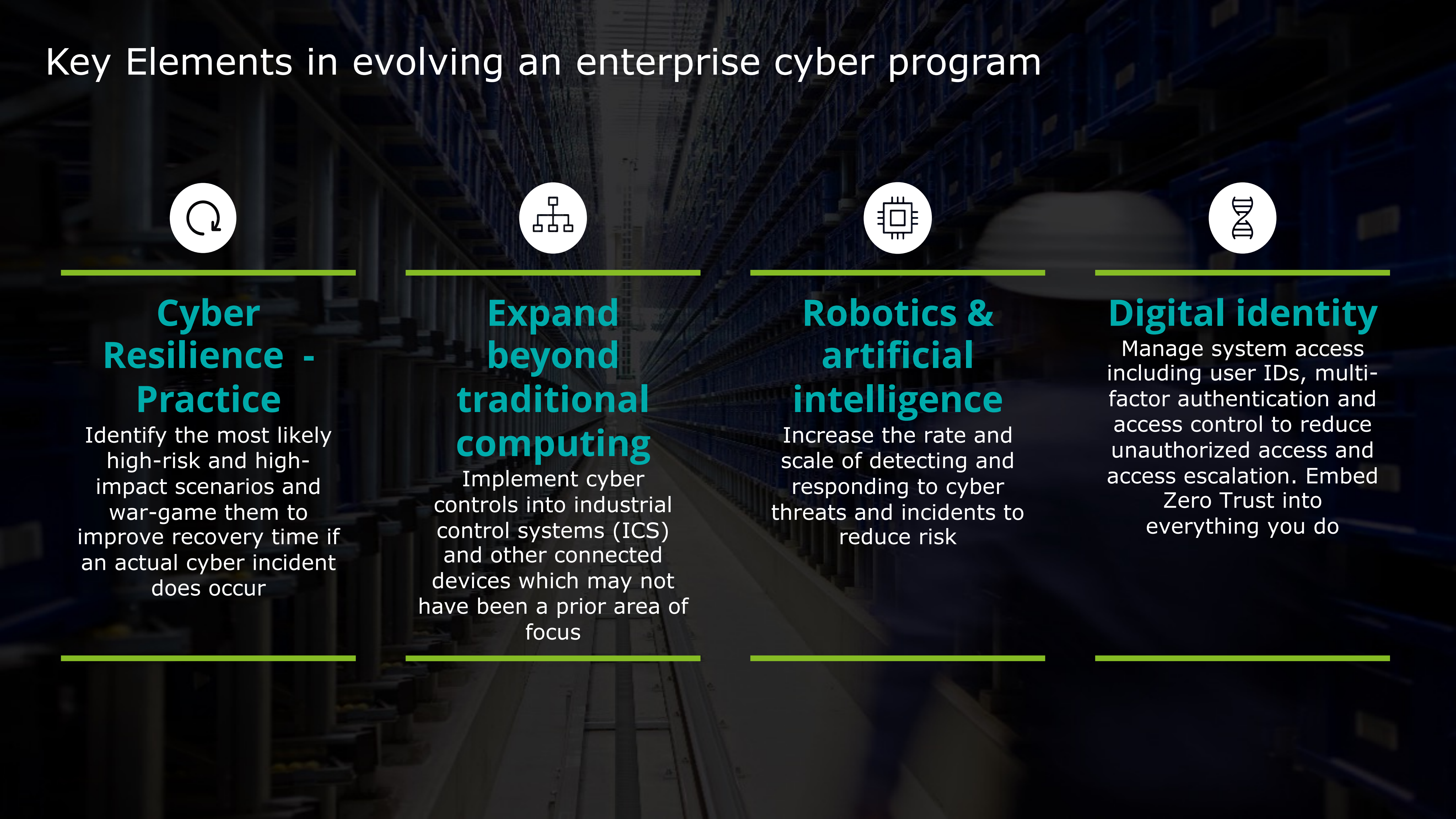
Cyber Terrorists

Cyber terrorists can target a whole range of businesses and do so by causing disruption and harm.

These types of attacks are on the rise and generally harass and stop businesses from running efficiently.

Cyber terrorists want to destroy organizations to bring awareness to their cause, for recruitment purposes, propaganda, financial gain, or political reasons.

Key Elements in evolving an enterprise cyber program



Cyber Resilience - Practice

Identify the most likely high-risk and high-impact scenarios and war-game them to improve recovery time if an actual cyber incident does occur

Expand beyond traditional computing

Implement cyber controls into industrial control systems (ICS) and other connected devices which may not have been a prior area of focus

Robotics & artificial intelligence

Increase the rate and scale of detecting and responding to cyber threats and incidents to reduce risk

Digital identity

Manage system access including user IDs, multi-factor authentication and access control to reduce unauthorized access and access escalation. Embed Zero Trust into everything you do

Cyber-centered questions CEOs should be asking

1. Do we demonstrate due diligence, ownership, and effective management of cyber risk?

2. Do we have the right leader and organizational talent?

3. Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?

4. Are we focused on, and investing in, the right things? And, if so, how do we evaluate and measure the results of our decisions?

5. How do our cyber risk program and capabilities align to industry standards and peer organizations?

6. Do we have a cyber-focused mindset and cyber-conscious culture organization wide?

7. What have we done to protect the organization against third-party cyber risks?

8. Can we rapidly contain damages and mobilize response resources when a cyber incident occurs?

9. How do we evaluate the effectiveness of our organization's cyber risk program?

10. Are we a strong and secure link in the highly connected ecosystems in which we operate?

Set the tone at the top

Institute a metrics driven conversation between the CEO/Board and IT

Illustrative

Yearly

Cybersecurity Program
- Effectiveness of cybersecurity program
- Cybersecurity maturity
- Industry benchmarks

Information Security Risks
- Risk appetite
- Audit findings
- Remediation status

Financial Elements
- Cyber security program budget
- Cyber risk transfer strategy against cyber security budget and financial exposure

Quarterly

Risk Reduction

reduction activities and their status
- Security of third-party suppliers/providers
- Exceptions management (for exceptions to identified security guidelines/standards

Financial Impacts
- Measurement of cybersecurity investments and their reduction in financial exposure (ROI)
- Metrics related to BUs and operating environments
- Cybersecurity budget analysis, including external (comparison to industry) and internal (security initiatives proposed, funded and trade-offs)
- Financial impact related to worst-case scenario

Ongoing (Operational)

Vulnerability Management, e.g.,
- # of unpatched vulnerabilities
- Aging status (tickets)

Attack Surface, e.g.,
- # of blocked attacks
- # of legacy applications waiting to be updated

Data Protection, e.g.,
- # of data incidents
- Data loss prevention metrics

Detection and Response, e.g.,
- Amount of time it takes to discover and respond to a cyber risk

Training and Awareness, e.g.,
- Phishing click rate, highlighting repeat offenders and business units with higher stats
- # of employees, contractors and temp workers that have finished training