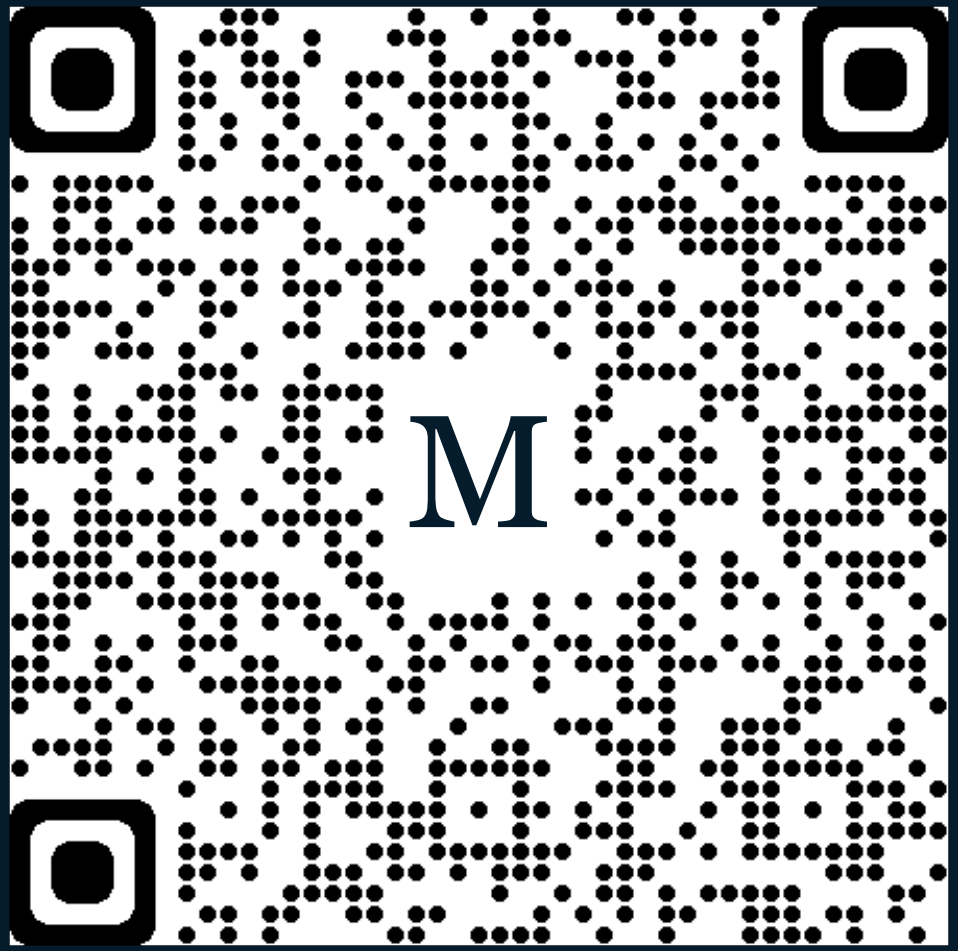
McKinsey & Company

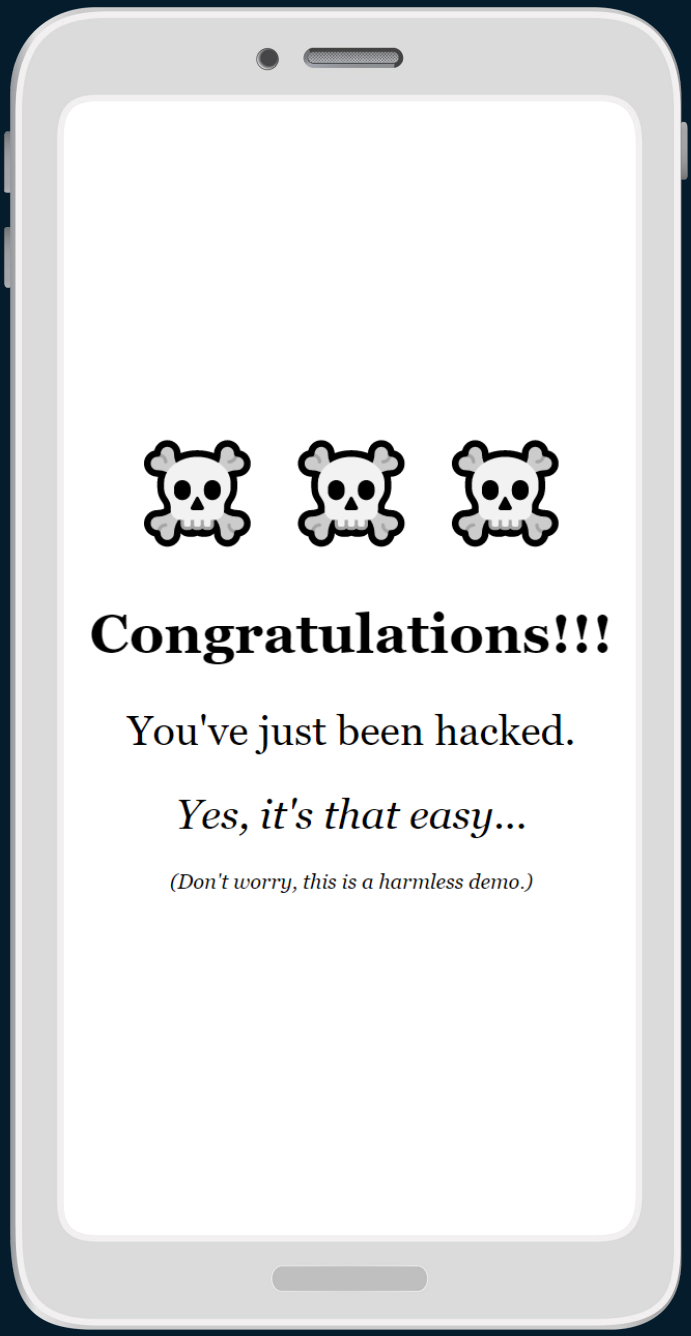
Futureproofing Cybersecurity

Institute of International Finance (IIF)
Special EMAC Session

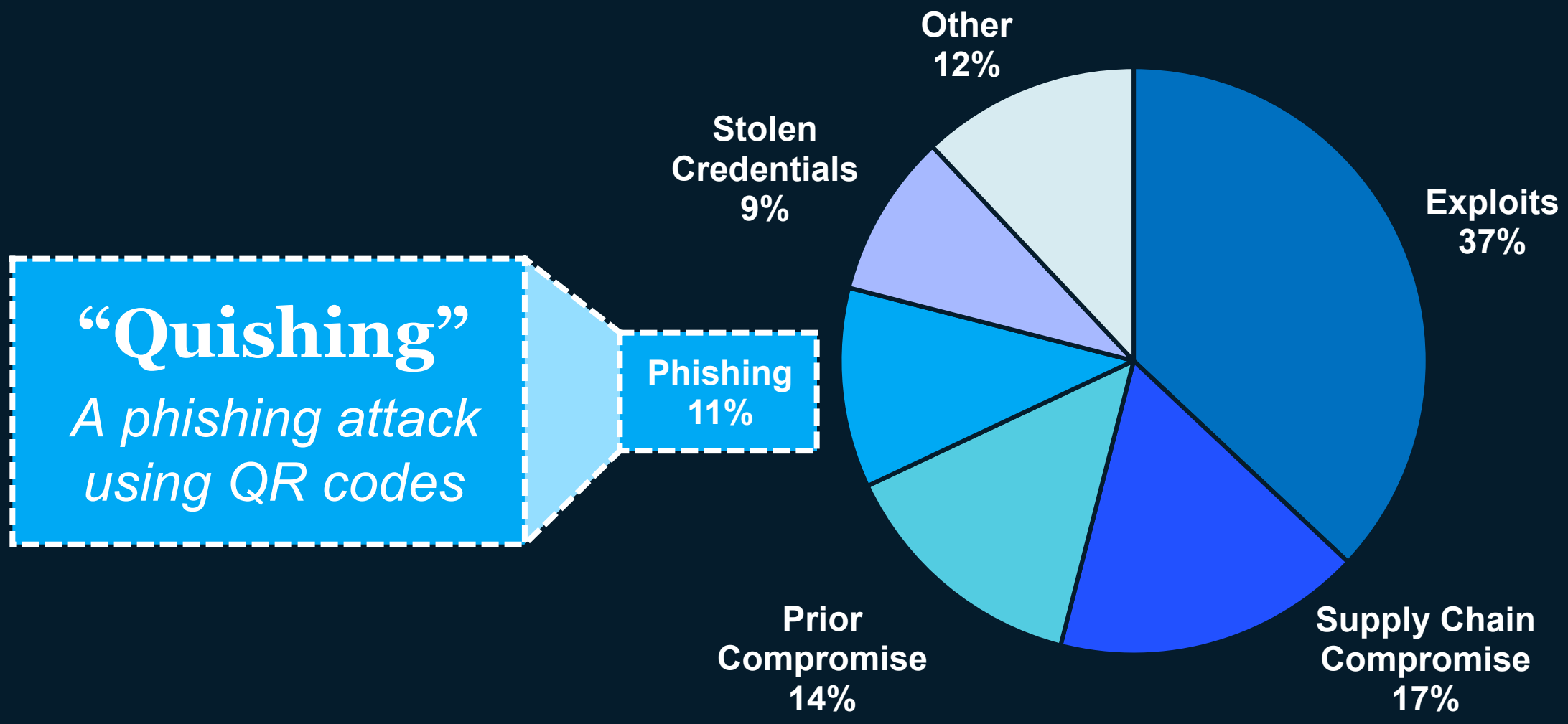
June 29, 2022

Please scan this QR code to download the digital material and follow along.



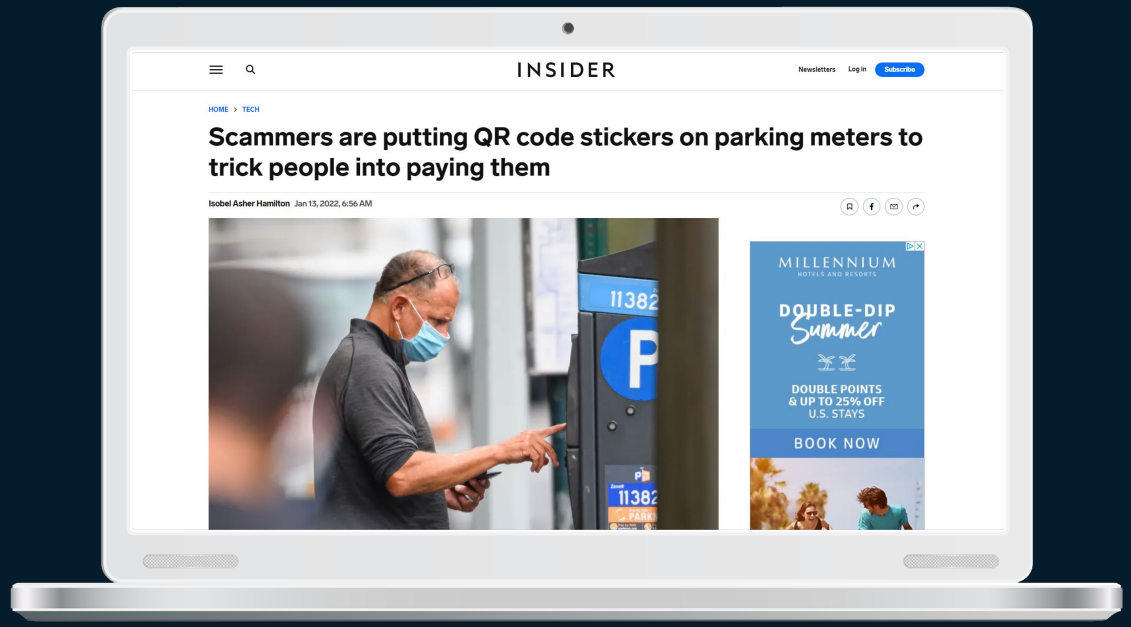

Congratulations!!!
You've just been hacked.
Yes, it's that easy...
(Don't worry, this is a harmless demo.)

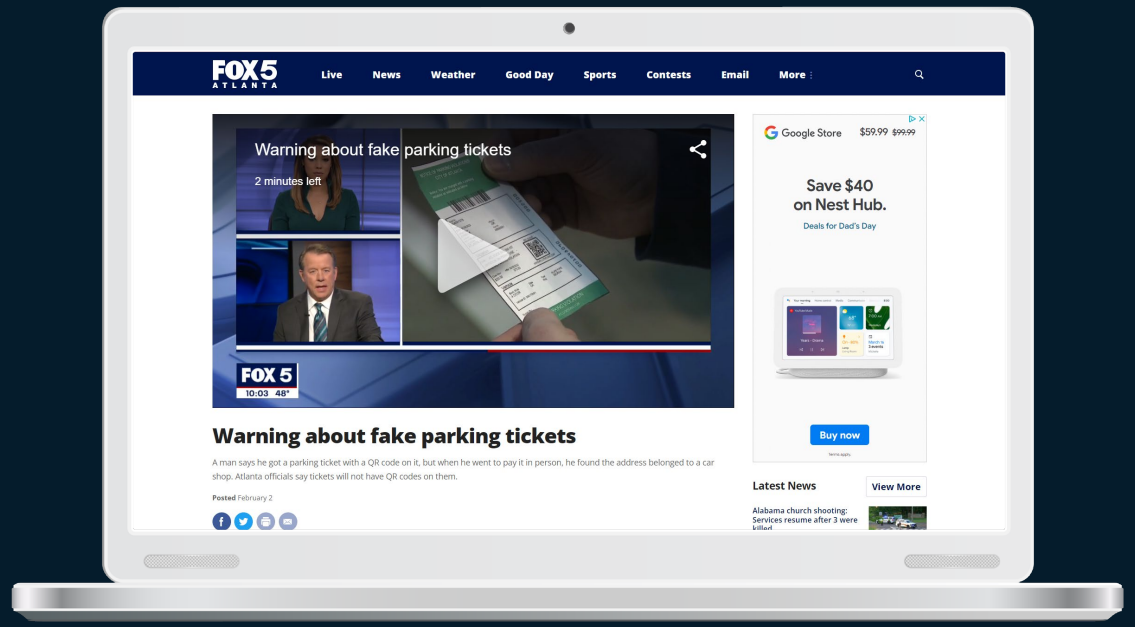
Cybersecurity risk is everywhere, and phishing remains a top attack technique.



Source: Mandiant MTrends Report 2022

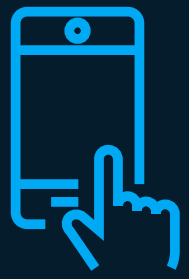
Law enforcement in Texas and Georgia warned of fraudulent QR code parking ticket payment links.



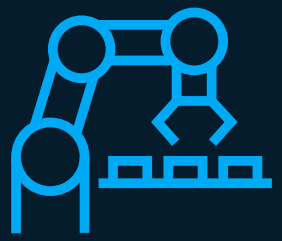


Source: (1) Business Insider, (2) Fox 5 Atlanta

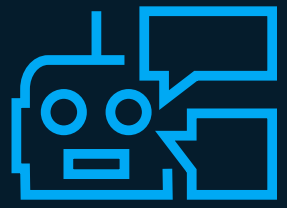
Companies continue to transform and modernize…



Mobile Apps



Connected Sensors



Artificial Intelligence

Cloud Computing

…and many more.

…increasing the cyber attack surface.

82%

…increase in ransomware-related data leaks in 2021[1]

Source: (1) CrowdStrike 2022 Global Threat Report

Today's attackers are well-funded, highly organized, and well-trained cyber criminals.

eCrime 49% ▼ 3%

Financially motivated criminal activity

Targeted 18% ▲ 5%

State-sponsored intrusion activity, espionage, or destructive attacks

Hacktivist 1% — NC

Attacks to gain momentum, visibility or publicity for a cause or ideology

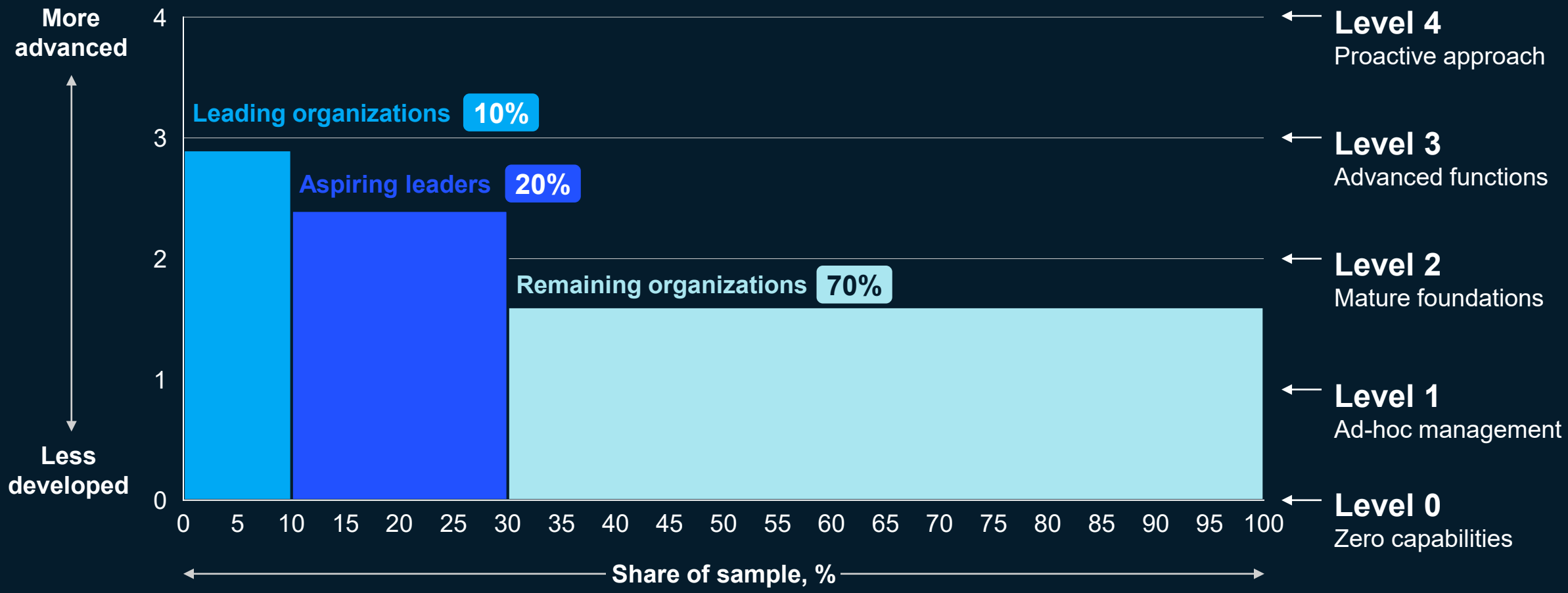
Unattributed 32% ▼ 2%

Insufficient data to make a confident attribution

Targeted threat actor groups origin country: Russia, Vietnam, North Korea, South Korea, Iran, Pakistan, Georgia, Columbia, China, India, Turkey

Source: CrowdStrike 2022 Global Threat Report

Companies struggle to invest in cybersecurity at-pace with the rising threat.



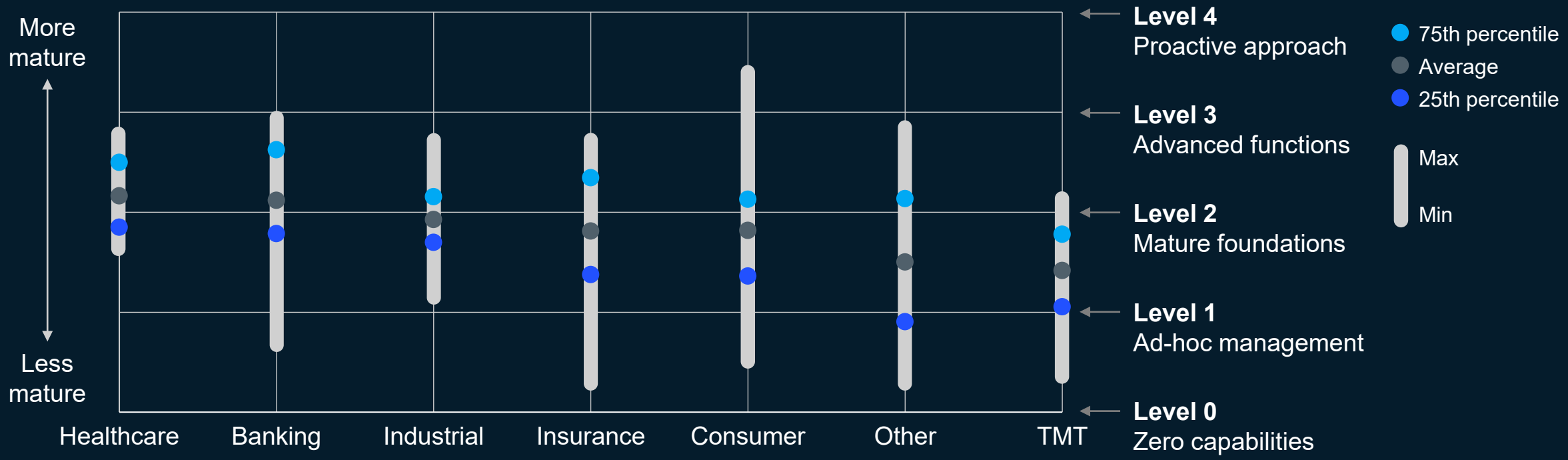
Cybersecurity maturity level survey, score (0 = low, 4 = high) (n = 114)

Source: McKinsey & Company, “Organizational cyber maturity: A survey of industries”

Industry matters when it comes to cybersecurity maturity.

Cybersecurity maturity varies within sectors more than it varies from sector to sector

Cybersecurity maturity level, industry sector breakdown, score (0 = low, 4 = high) (n = 114)



Healthcare and banking are the sectors with the best overall cybersecurity-management profiles, as more than half the companies in each of these sectors have a maturity level of 2 or above; however, maturity levels still vary widely within each sector

Source: McKinsey & Company, "Organizational cyber maturity: A survey of industries"

Lack of investment in cybersecurity can result in breaches, disruption, and disaster.

	2019	2021	2021
	Financial services firm	**Insurance carrier**	**Energy supplier**
Attack impact	Personal info of +100M credit card customers/ applicants	Cyber attack shut down critical business systems and 75K records were stolen	Utility shut down to contain IT breach; fuel shortages in eastern United States
Nature of breach	Misconfigured web application firewall (WAF) to access AWS S3 servers	Double extortion ransomware attack; $40M ransom paid to threat actors	Compromise of billing system via VPN; $4.4M ransom demands

Regulation is increasing and forcing companies to disclose cybersecurity breaches.

1 **Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)[1]**

16 critical infrastructure sectors[2]

2 **United States Security Exchange Commission (SEC) Cyber Disclosure Rule[3]**

Publicly listed U.S. companies

What does this mean for companies today?

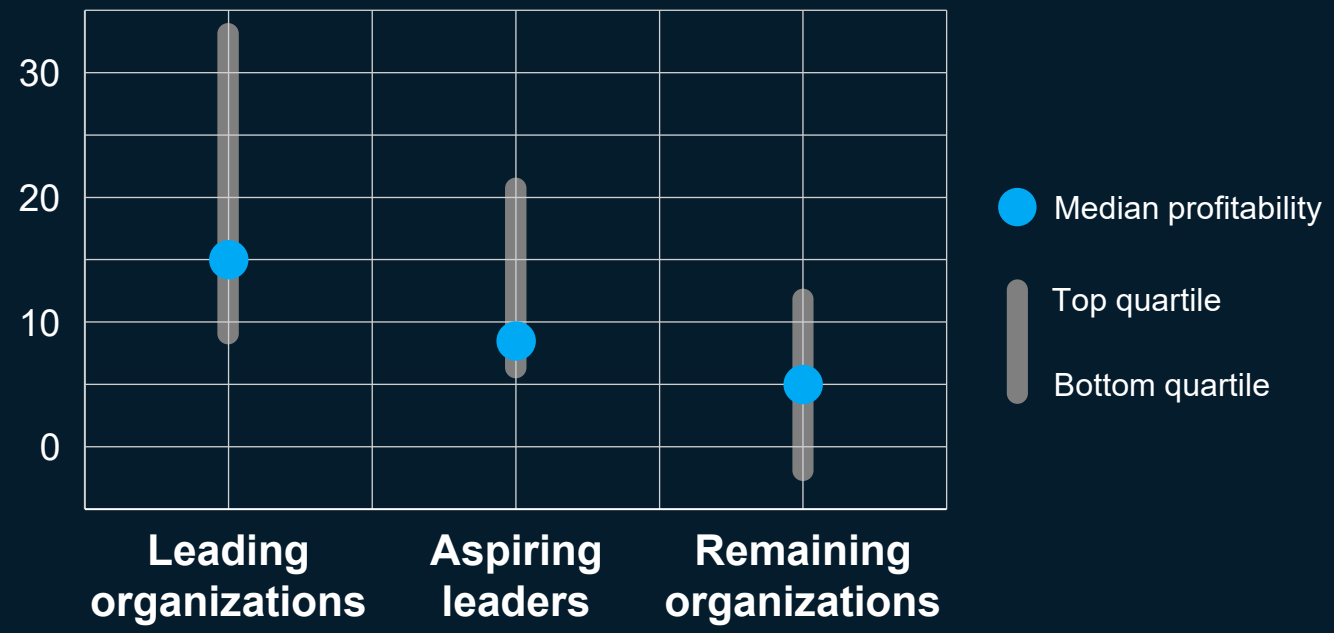
- **Board training and expertise**
- **Increased reporting**
- **Investor, customer, and vendor scrutiny**
- **More questions for the CISO/CIO**
- **Stronger detection and response capabilities**
- **Enhanced preparation and training**
- **Investment in cyber program**

Other countries are considering or implementing similar cybersecurity disclosure guidelines, such as India[4].

Source: (1) CIRCIA; (2) Critical infrastructure sectors; (3) SEC Cyber Disclosure Rule; (4) CERT-In Directives [Reuters, CSO]

Cybersecurity can create a competitive differentiator that helps companies accelerate their mission and protect their purpose.

Profitability in last fiscal year
% average net margin



Key Takeaway

More profitable companies build stronger cybersecurity programs.

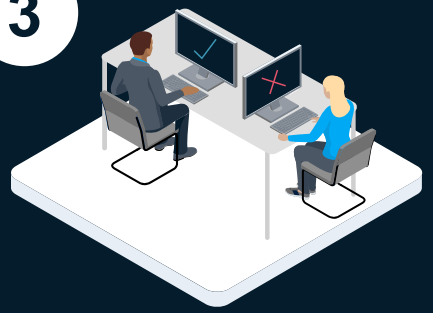
Source: S&P Capital IQ; McKinsey Cybersecurity Maturity Survey 2021

Strong cybersecurity creates competitive advantage.

1 Strategy, Program Mgmt, & Performance

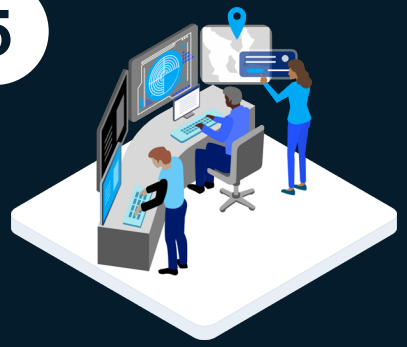
2 Governance, Risk, and Compliance

3 Identity and Access Management



4 Architecture and Engineering

5 Security Operations and Response



6 Cyber Resilience and Recovery

7 Data Protection and Privacy

8 Physical Security and Safety

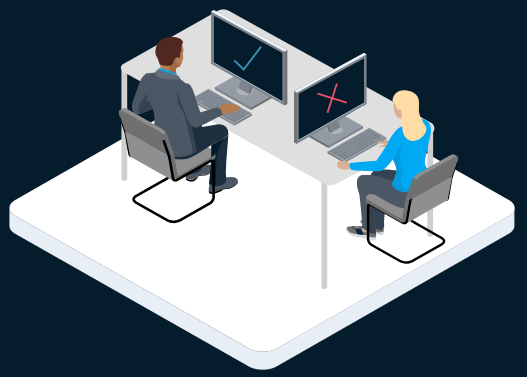
Each cyber capability has a set of sub-capabilities.
(1 of 2)

1 Strategy, Program Management, & Performance

Security Strategy	Security Project and Program Management	Security Service and Product Management
Financial Management	Talent Management	Security Team Learning and Development
Security Vendor Management	Business Relationship Management	Communications Management
Metrics and Reporting		

2 Governance, Risk, and Compliance

Security Governance	Policies and Standards	Training, Education, and Awareness
Third-Party Security Risk Management	Supply Chain Security	Security Risk Management
Digital Trust and Safety	Security Assurance	Security Compliance
M&A Security	Cyber Insurance	Insider Threat Program



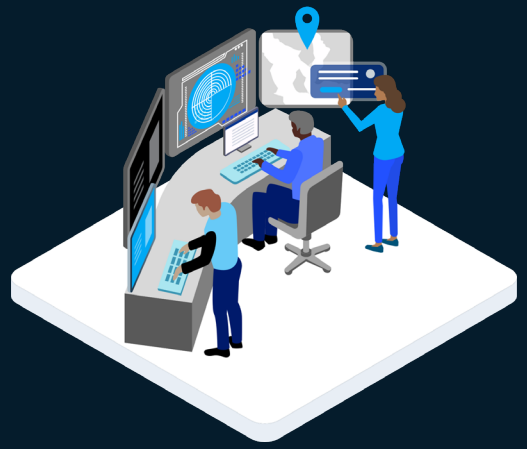
3 Identity and Access Management

Identity Management	Access Management	Identity and Access Governance
Privileged Access Management	Cryptography and Key Management	Fraud

4 Architecture and Engineering

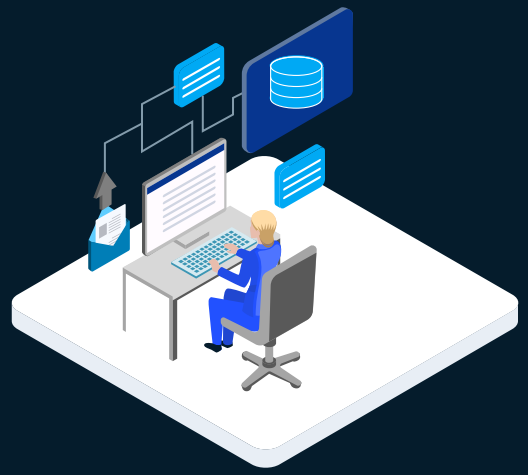
Security Architecture	Security Engineering and Integration	Security Infrastructure and Tooling
Operational Technology Security	Cloud Security	Network and Communication Security
Secure Software and Product Development	IT Asset Management	Security Consulting and Advisory
Edge and IoT Security	Emerging Technologies and Innovation	Threat Modeling

Each cyber capability has a set of sub-capabilities.
(2 of 2)



5 Security Operations and Response

Threat and Vulnerability Management	Threat Intelligence	Security Logging and Monitoring
Security Incident Response	Application Security Testing	Endpoint Security
Security Automation and Orchestration	Patch Management and Remediation	Threat Hunting and Active Defense
Forensics and Investigations		



6 Cyber Resilience and Recovery

Cyber Crisis Readiness	Cyber Crisis Response	Cyber Recovery and Restoration
Business Continuity Management	Disaster Recovery	

7 Data Protection and Privacy

Data Loss Protection	Data Lifecycle Management	Privacy Compliance
Privacy Operations	Encryption and Tokenization	

8 Physical Security and Safety

Facility Security and Physical Access Control	Surveillance and Monitoring	Physical Crisis Response
Environmental Protection	Personnel and Workforce Security	Executive Protection
Physical Asset Security		

Transforming cyber capabilities today can help futureproof against the scenarios of tomorrow.

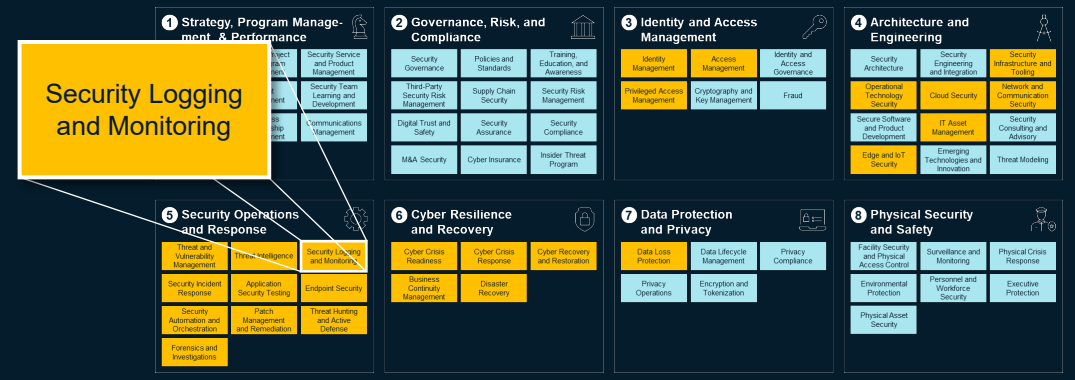
A Cyber Scenarios for Futureproofing

- Universal identity fraud
- Existential challenge to CISO org
- Cyber militarization
- Mass network rebuild
- Asset sprawl
- Multi-supply chains
- Quantum revolution
- Ubiquitous biometrics
- Algorithmic distrust
- Splinternet
- Digital pandemic

B Cyber Capabilities

- Strategy, Program Management, & Performance
- Governance, Risk, and Compliance
- Identity and Access Management
- Architecture and Engineering
- Security Operations and Response
- Cyber Resilience and Recovery
- Data Protection and Privacy
- Physical Security and Safety

C Cyber Transformation Recipes



A **11** cybersecurity scenarios will fundamentally challenge the organizations of tomorrow

B **8** core cybersecurity capabilities “power” cybersecurity organizations

C **67** sub-capabilities combine to form “recipes” for transformation and futureproofing

Cybersecurity futureproofing recipes…
(1 of 2)

Cyber transformation recipe	Impacted capabilities	Top 3 steps to take today
1. **Invest** in talent and empower your leaders		• **Leadership development programs** • Invest in strong cyber recruiting pipelines • Deploy technical upskilling/education program
2. **Know** your users and your nth party ecosystem		• **Invest in strong IAM capabilities** • **Inventory and risk-assess all third-parties** • Assess supply chain security and build resilience
3. **Defend** your assets and your data		• **Inventory your crown jewel assets and data** • Understand the privacy-related regulations • Implement strong encryption over sensitive data
4. **Build** trust by design (security, privacy, and compliance) into products and services		• **Develop strong DevSecPrivOps processes** • Create real-time compliance monitoring • Train and empower development/product teams
5. **Embed** deep within the business and products and services		• **Deploy BISOs & security champion program** • Measure/improve engagement and satisfaction • Build service-oriented, platform-enabled catalog

Cybersecurity futureproofing recipes…
(2 of 2)

Cyber transformation recipe	Impacted capabilities	Top 3 steps to take today
6. **Listen** to your environment and prepare to respond		• **Ensure completeness & depth of monitoring** • Create and exercise incident response playbook • Assess technical readiness/response capabilities
7. **Plan** for disruption and practice "from scratch" recovery		• **Perform cyber crisis simulations/wargames** • Build cyber crisis management program • Build extreme recovery/restoration capabilities
8. **Measure,** synthesize, and communicate in business terms		• **Build business-oriented board reporting** • Define the cyber metrics that matter • Educate board and provide ongoing updates
9. **Converge** enterprise, product, OT, and physical security		• **Assess OT assets & extend cyber controls** • Integrate physical and cybersecurity monitoring • Extend security controls to customer products
10. **Adopt** a cloud-first mindset and experiment with emerging tech		• **Build secure cloud landing zones & controls** • Integrate cloud security into IT/Business/products • Reward and recognize innovation with new tech

The future of cybersecurity will be shaped by the steps we take today.

Cybersecurity is key to building trust in the digital age

Cyber threats will continue to evolve and so too will the measures we use to protect our organizations

The steps we take today can help futureproof organizations against the threats of tomorrow

But in order to futureproof your cybersecurity, organizations must do two things…

1. **Know yourself** and the capabilities that make up your cybersecurity program

2. **Forecast the future** to assess the impact of future trends to your program and its capabilities

Q&A

McKinsey & Company

Thank you

Justin Greis

Partner, Chicago

Justin_Greis@mckinsey.com

linkedin.com/in/justingreis

Twitter: @JustinGreis