McKinsey & Company

Cybersecurity and the Board of Directors

Boardroom Summit & Peer Exchange

September 16, 2022

Introductions

Justin Greis

Partner, Chicago

McKinsey Cybersecurity leader focused on building secure and trusted organizations

Brian Kelly

Senior Advisor, Wilmington

Former Chief Security Officer – Rackspace; Advisory Board Member, Splunk, Crowdstrike, InQuest and TruStar

Agenda

Why does cybersecurity matter?

15 mins

Gain an understanding of the current landscape of cybersecurity and cyber crime, including

- The growing attack surface
- Ransomware as a Service
- Cybersecurity trends and maturity
- Recent cybersecurity attacks

How do boards engage with cybersecurity?

15 mins

Discuss potential means of engagement with cybersecurity for the board including

- Questions the board should be prepared to ask regarding cyber
- Roles the board can take to support cybersecurity

What does effective cybersecurity look like?

10 mins

Discuss essential cyber capabilities including

- Descriptions, objectives, and NIST dimensions covered for eight essential cyber capability groups
- Steps companies can take now to “futureproof” their cybersecurity capability

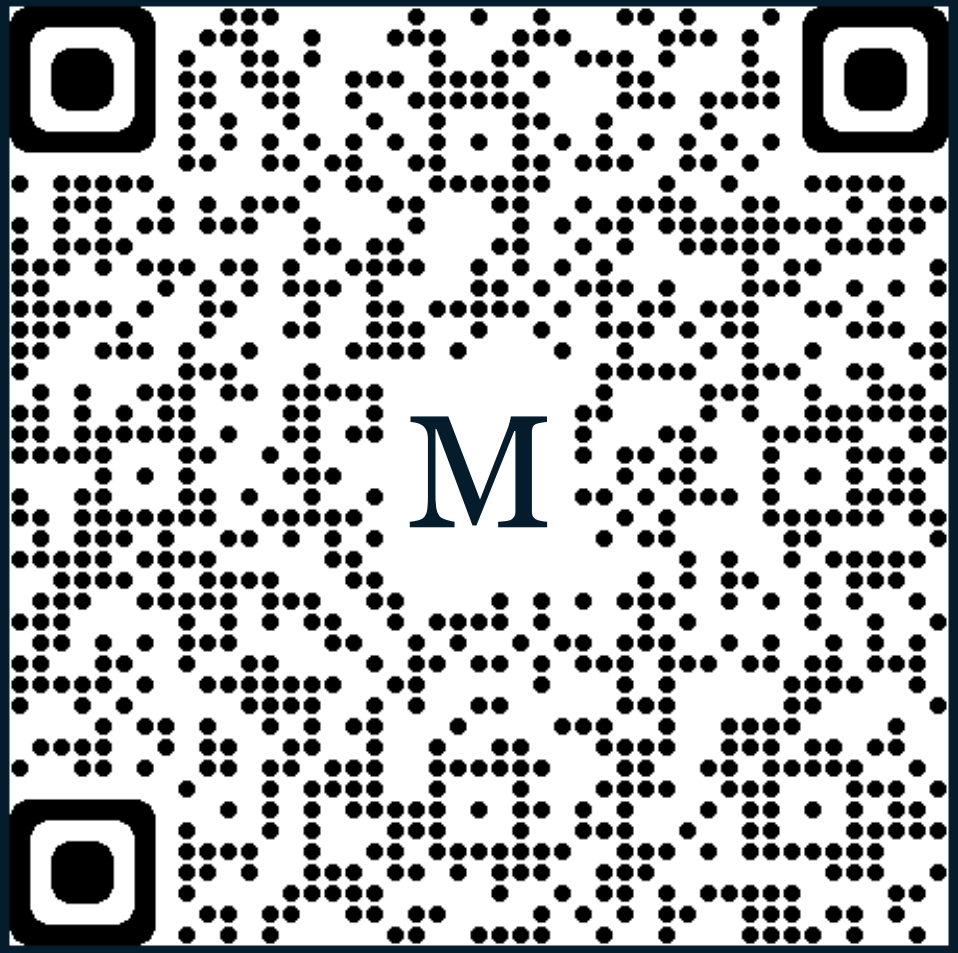
---

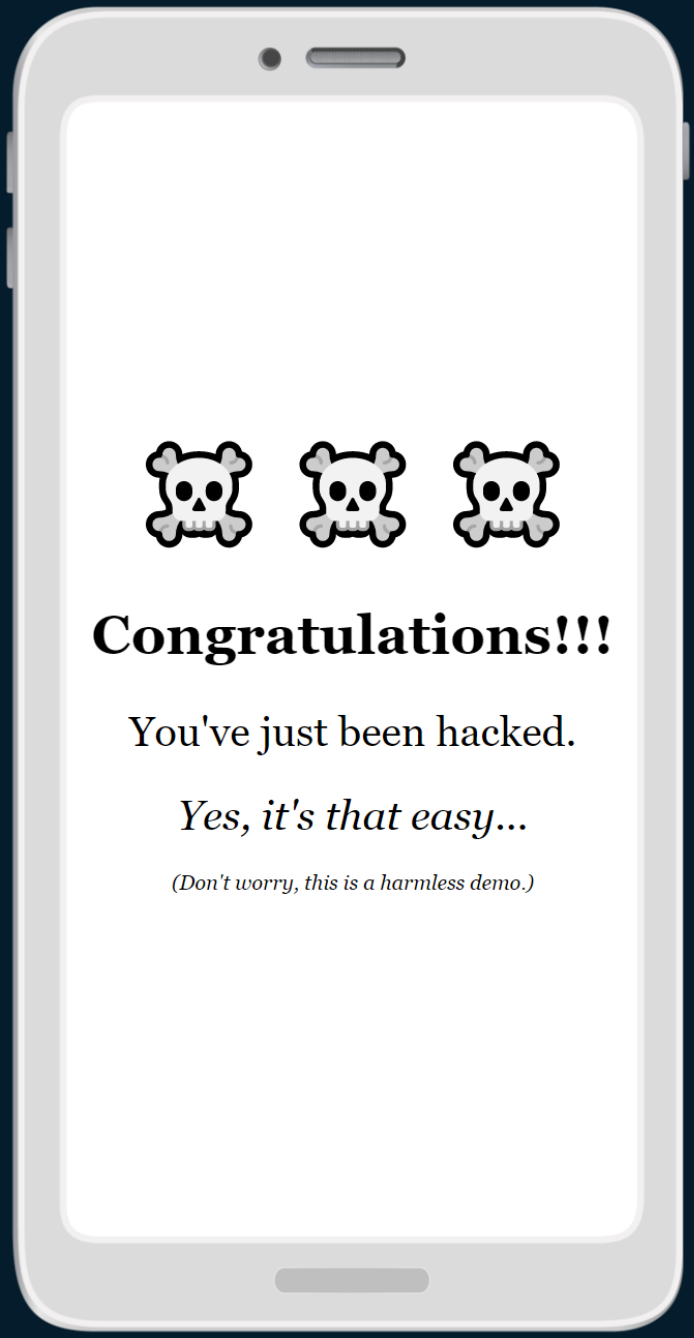
Q&A

10 mins

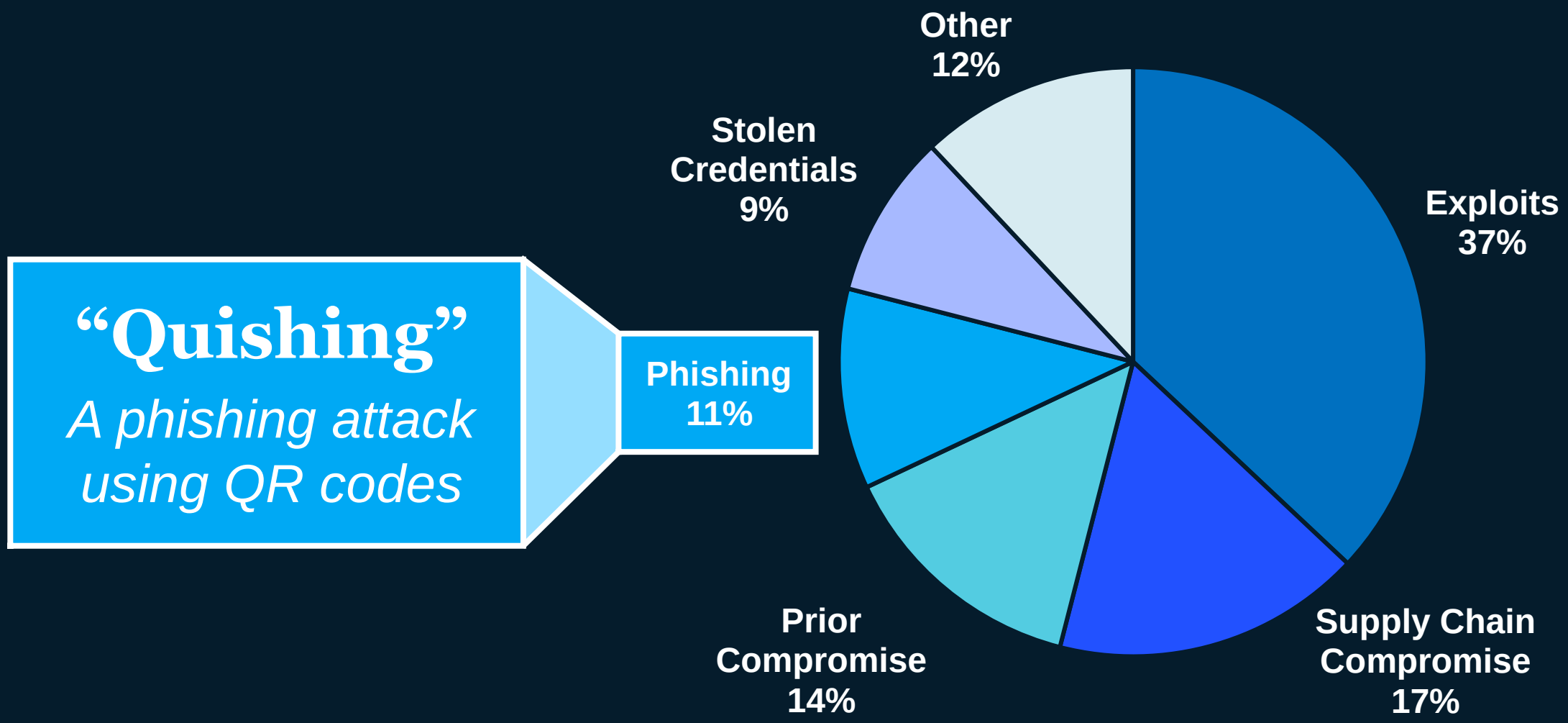
Feel free to ask questions throughout the session

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



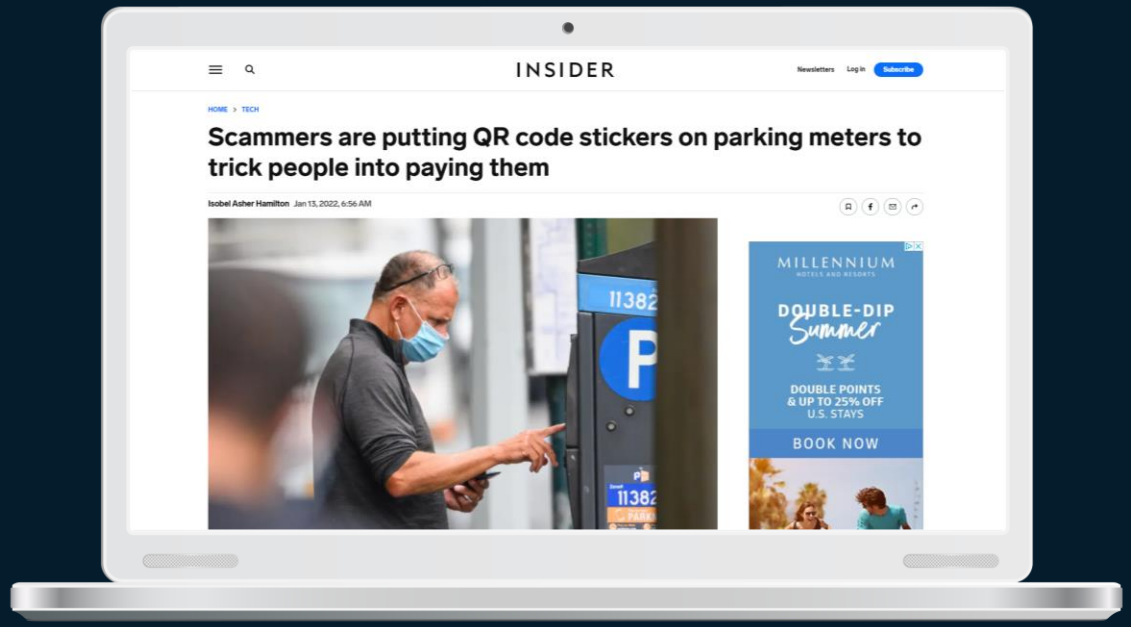

Congratulations!!!
You've just been hacked.
Yes, it's that easy...
(Don't worry, this is a harmless demo.)

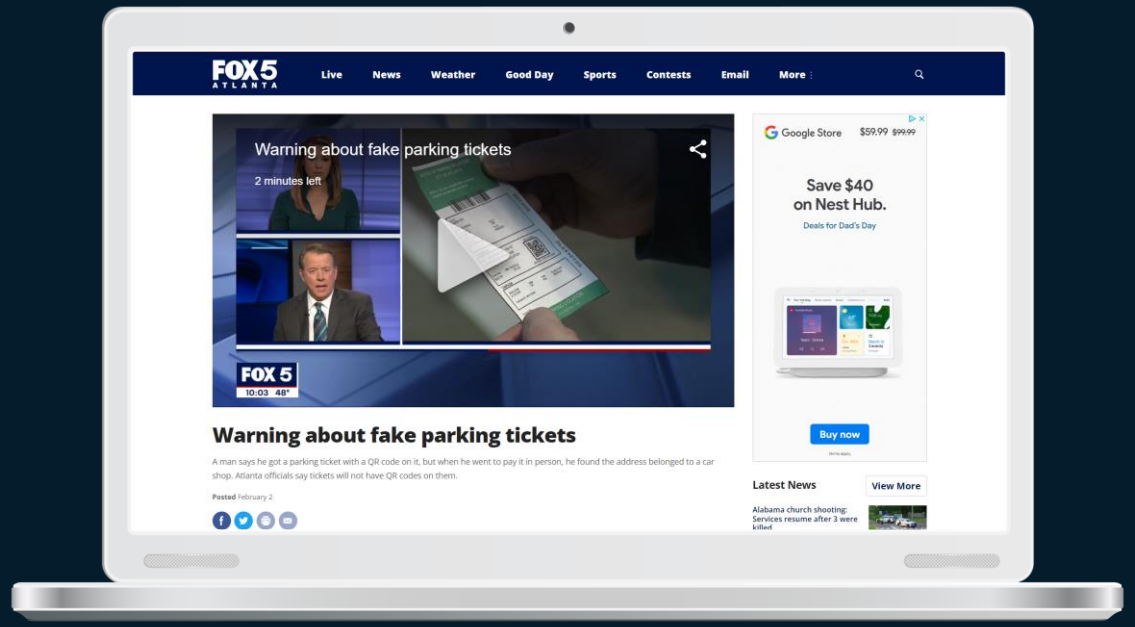
Cybersecurity risk is everywhere, and phishing remains a top attack technique.



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

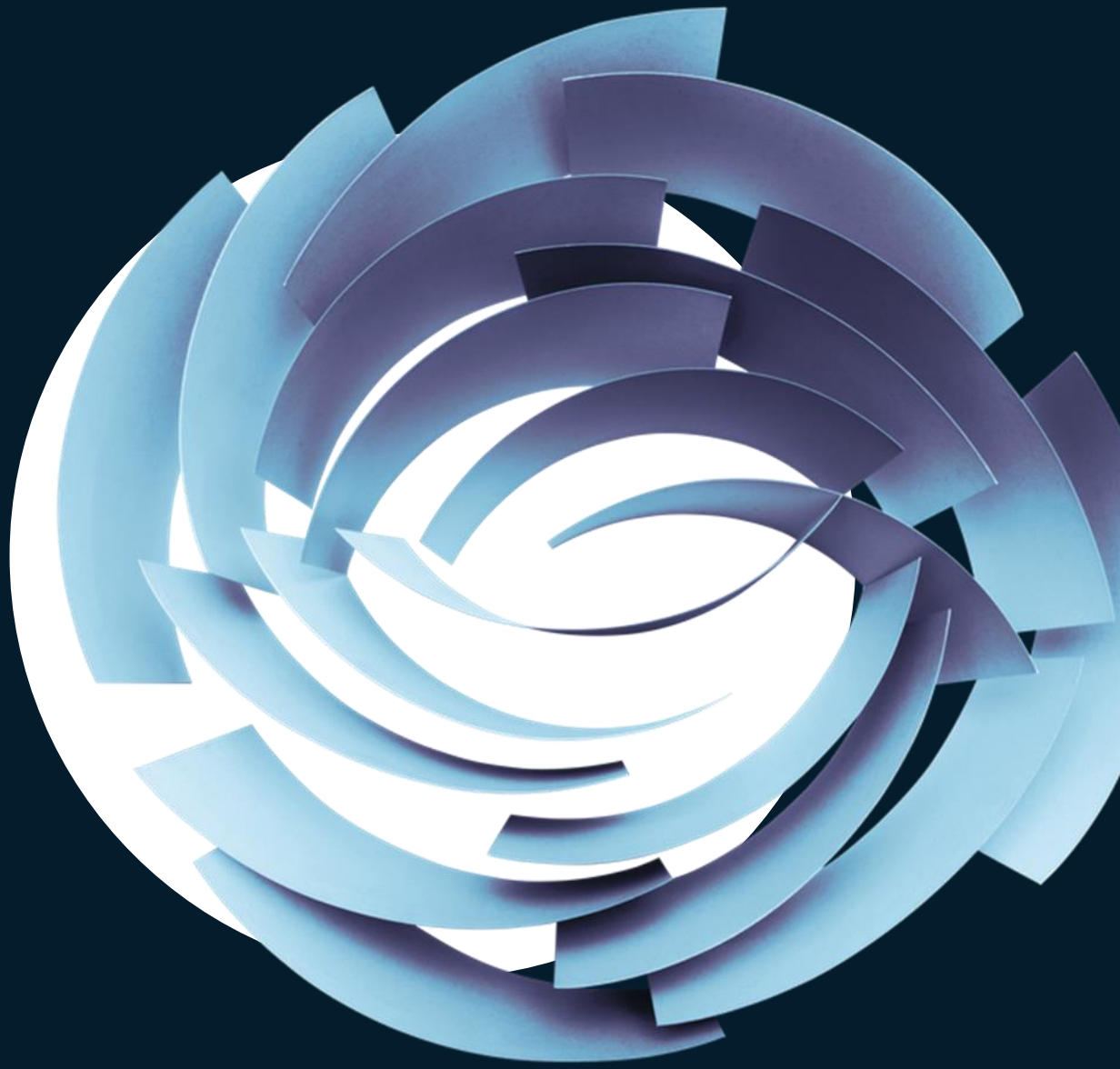
Agenda

Why does cybersecurity matter?

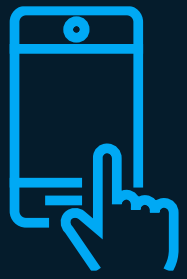
How do boards engage with cybersecurity?

What does effective cybersecurity look like?

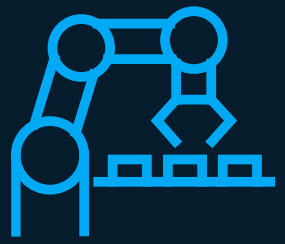
Q&A



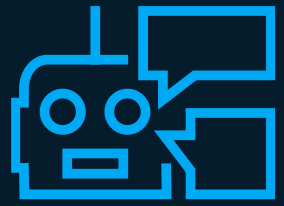
Companies continue to transform and modernize…



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

The cybersecurity attack surface grows with increasing digitization, connectivity and migration to cloud

1. **Information Technology (IT) / Operational Technology (OT)**

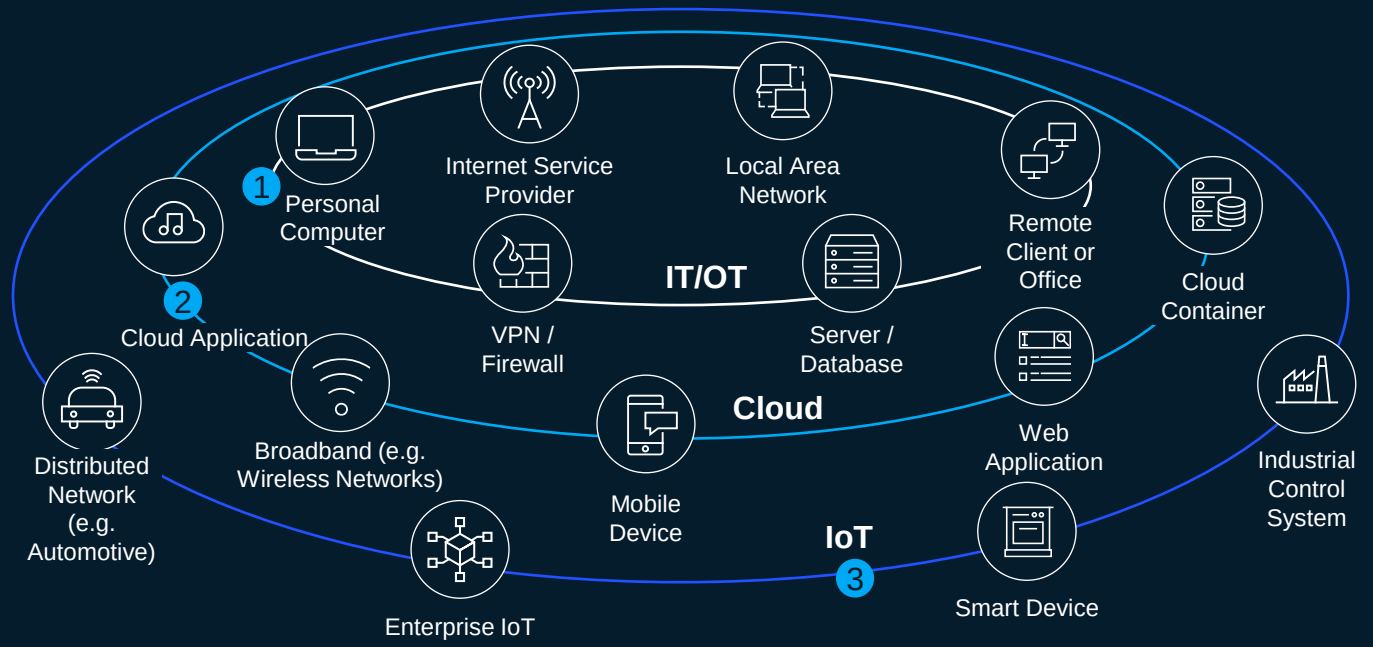
   IT / OT includes all corporate owned and managed systems, including both computers and machinery.

2. **Cloud / External Supplier systems**

   Security and privacy introduce unique challenges as cloud providers often have responsibility for maintenance and operation of security controls

3. **Internet of Things (IoT)**

   Internet of things are systems of interconnected computing devices which communicate with one another without the need for human interaction.



Attack surface refers to the sum of systems and applications that can be exploited to carry out a cybersecurity attack.
One method of reducing the impact of a cyber-attack is to reduce the attack surface of a given system or organization.

Impacts of growing attack surfaces can be seen through increase in ransomware

Ransomware has exploded due to broad opportunity (e.g., poor cyber hygiene at many institutions), easy access and use of Ransomware as a Service, and availability of cryptocurrencies

The majority of ransomware attacks now **include data exfiltration** and **extortion**, and **exfiltrated data is increasingly made public or destroyed**

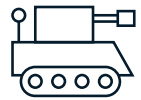
Key insights

- Over 75% of ransomware breaches begin with either a **phishing email** or **remote desktop compromise**
- Ransomware often **exploits unpatched vulnerabilities** and **credential compromise**
- **"Whether to shut down the network"** is an ongoing question for leadership
- Paying the ransom is **not a guarantee for data recovery or immunity from future attacks**

Source: Coveware Quarterly Ransomware Reports for Q4 2020 and Q1 2021; Source: Industry and Law Enforcement Interviews; FireEye, "Ransomware: Attacker's top choice for cyber extortion," link; FireEye Mandiant, "M-Trends 2021, Special Report," link

While companies continue to improve internal cyber hygiene, companies should also consider…

Understand required disclosures, notifications, and other legal requirements



Wargame a potential ransomware attack

Make practical preparations for a potential attack, e.g., build an escalation pathway

Low technical barriers for entry and profitability have boosted RaaS business

What is RaaS?

RaaS, Ransomware-as-a-service, is a **subscription-based model** that enables affiliates to use already-developed ransomware tools to execute ransomware attacks.

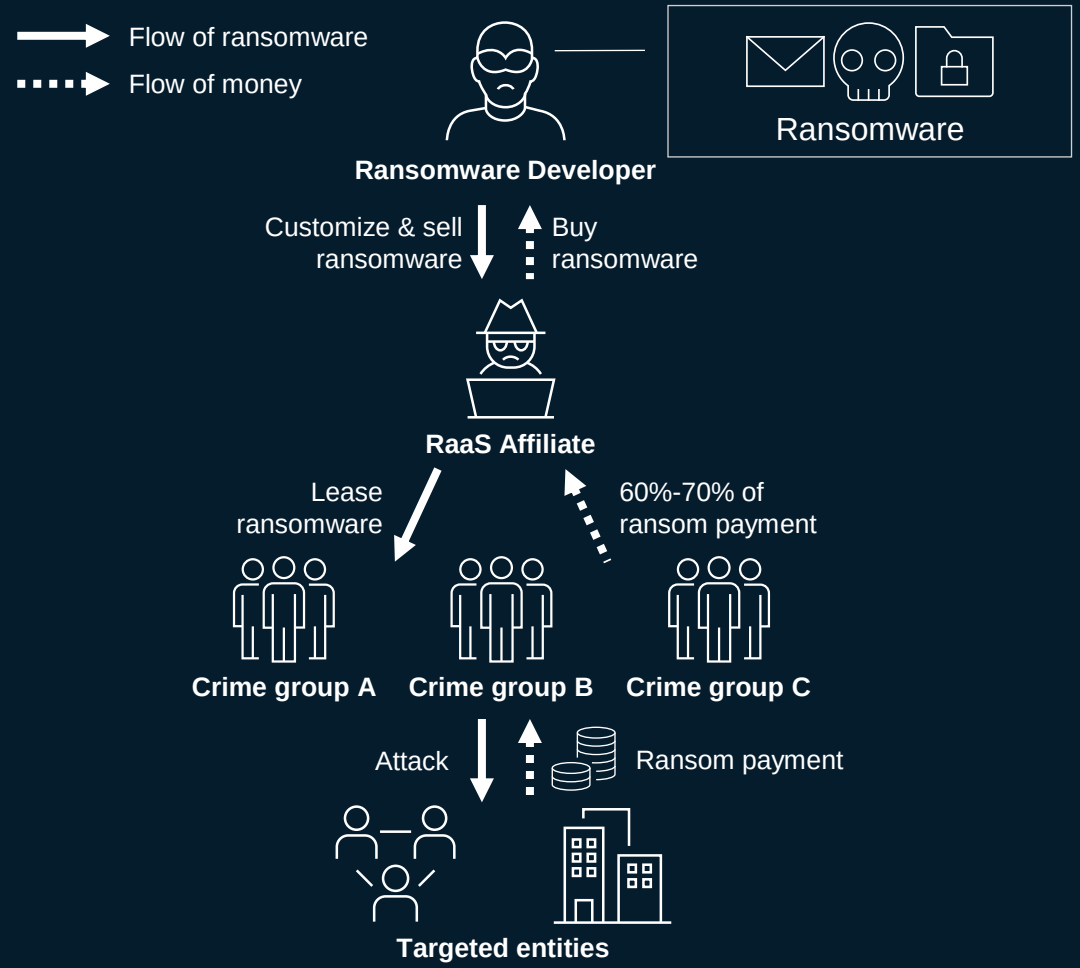
RaaS business started around 2017, and the **number of ransomware sold in the dark web has been increasing** ever since

The cost of a compromised corporate RDP credential is as little a $3 USD, and an effective full RaaS package can be bought for as low as $50 USD

Features of RaaS

- **Low technical barrier of entry for users** – Like all SaaS solutions, RaaS users don't need skills or experience to start the ransomware attack. Also, the license fee is set low that the service is easy to reach for any crime groups.
- **Prodigious affiliate earning potential** - it pay their affiliates very high dividends, usually 60-70% of total ransom paid by the targeted entities.

Ecosystem of ransomware



Source: What is Ransomware as a Service (RaaS)? The Dangerous Threat to World Security, UpGuard,2021

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

eCrime

Financially motivated criminal activity

49% ▼ 3%

Targeted

State-sponsored intrusion activity, espionage, or destructive attacks

18% ▲ 5%

Hacktivist

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

1% — NC

Unattributed

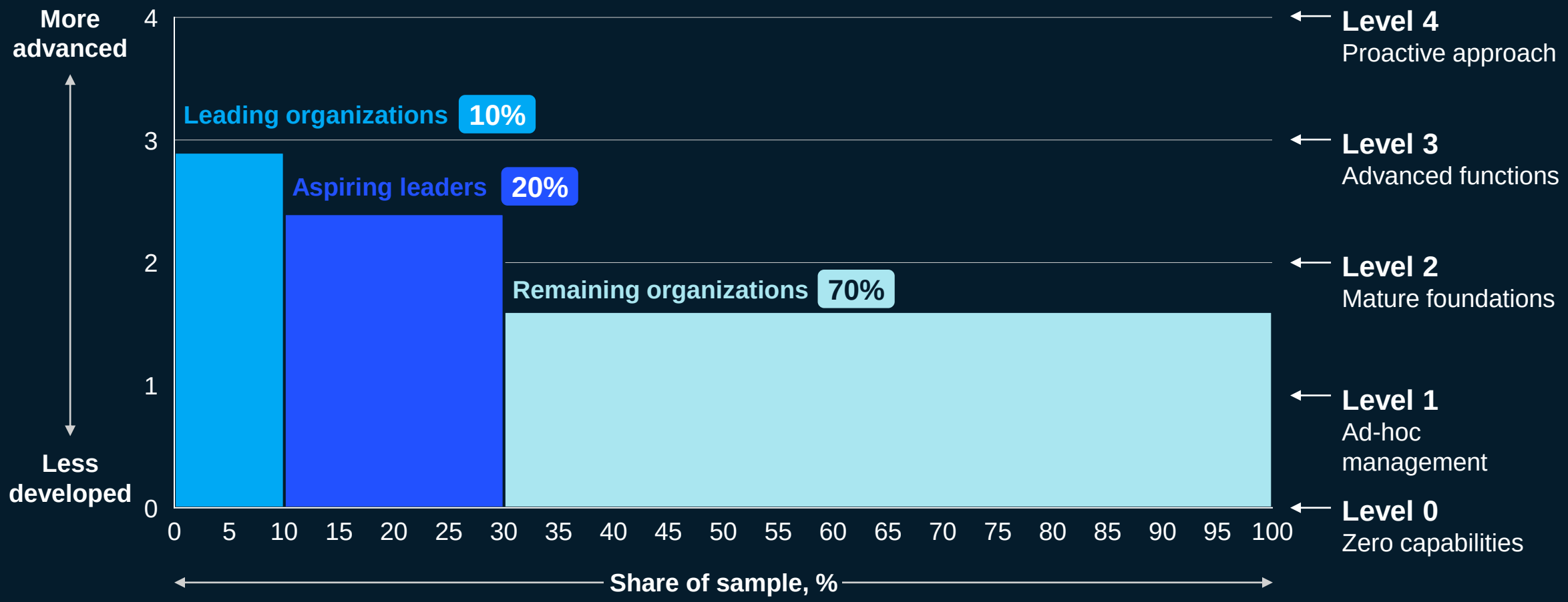
Insufficient data to make a confident attribution

32% ▼ 2%

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



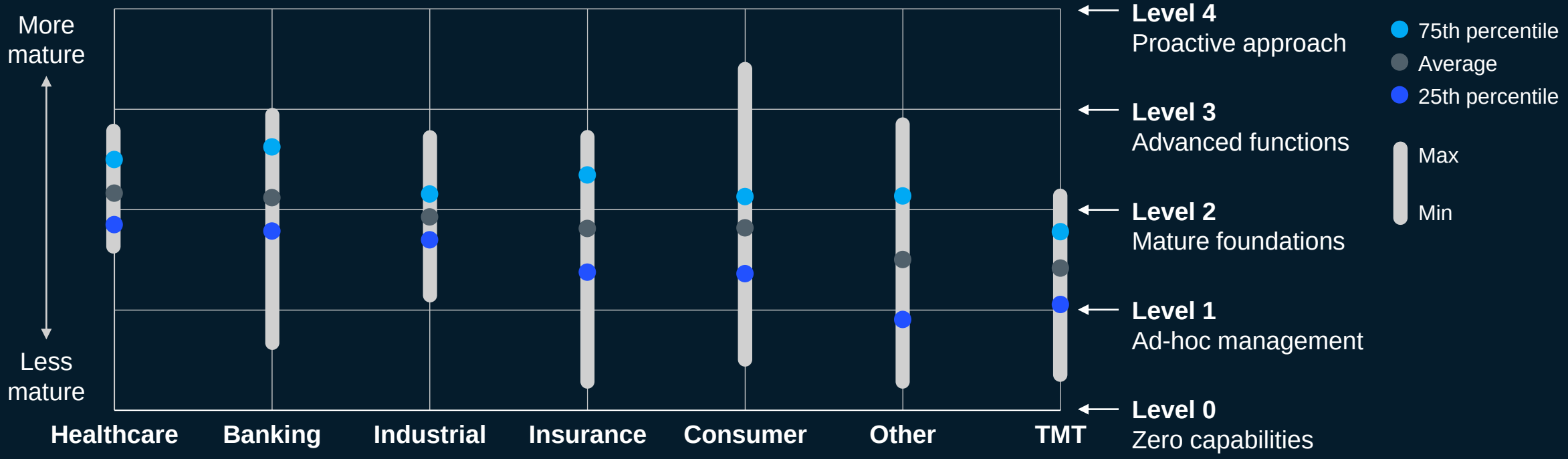
Cybersecurity maturity level survey, score (0 = low, 4 = high) (n = 114)

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"

Recent attacks demonstrate a variety of attack types

	Consumer goods manufacturer	Food processer	Energy supplier
Attack impact[1]	**2019:** Payment information of customers may have been stolen	**2021:** Cyber attack temporarily shut down food processing operations	**2021:** Pipeline shut down to control IT breach; fuel shortages in eastern US
Nature of breach[1]	"Unauthorized" malicious code on company website led to stolen data	Ransomware attack; $10M+ ransom paid to threat actors	Compromise of billing system via VPN; $4.4M ransom demands

1. All information based on publicly available and reported data

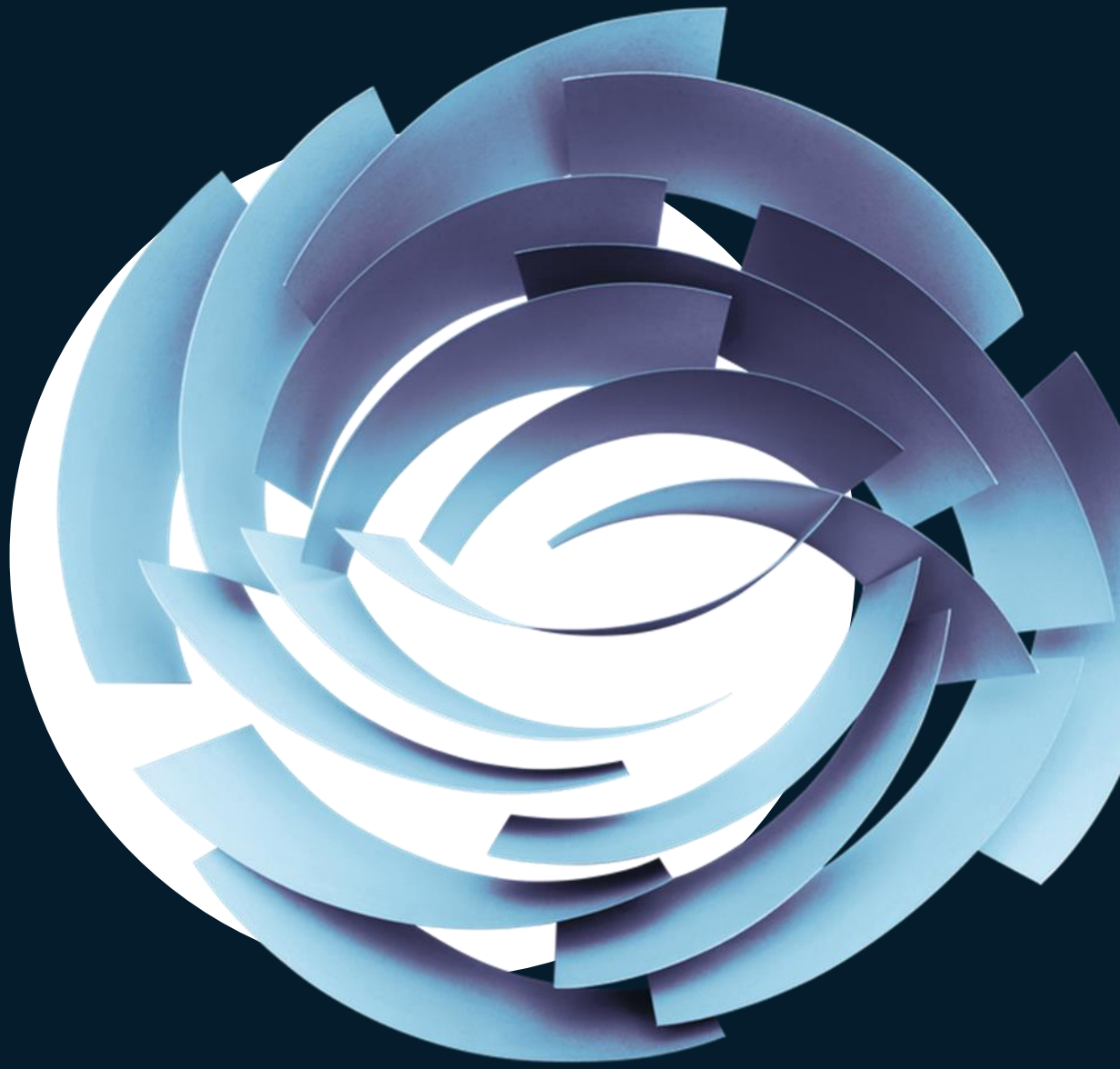
Agenda

Why does cybersecurity matter?

How do boards engage with cybersecurity?

What does effective cybersecurity look like?

Q&A



For the most part, Boards tell us they are not getting what they expect on cyber – and they are increasingly concerned

What we hear from boards…

Basic cyber education is not effective	"… don't know anything about cyber, I don't even know what questions to ask"
Too much data and too little real insights	"The documents we get are simply too long to absorb and digest"
Communication is not well structured	"I can't tell what is important and where I should focus my attention"
Metrics presented are difficult to interpret	"Not clear how the numbers tie to real risk levels, I wonder how we are really doing in cyber"
Progress difficult to identify and measure	"Doesn't look like we're seeing any progress in buying down risk"
Leadership role is unclear	"Rarely do we get anything beyond an ask for nominal approval of proposed policies"

Boards can actively engage cyber leaders in a few key ways

Helpful activities for Board Members

Participate in cybersecurity **Board education sessions**

Review and challenge 3rd party security reviews

Become very **familiar with internal measurements** and compare them to external data for benchmarking

Participate in table-top exercises to talk through the **key risks and how a cyber incident can be managed**

Designate a Non-executive Director as the **lead "owner" for cyber**

Ten good questions Boards should ask their CISOs

1. Where are we **most vulnerable** to cyberattacks? How long does it take to identify and remediate/patch vulnerabilities?
2. What percentage of our environment are we **logging and monitoring** for suspicious activity? Are there any areas we don't have good monitoring and detection visibility?
3. **Who would we call**, and in what order, if we were under attack? Do we have the appropriate retainers/contracts in place? (e.g. legal, forensics, crisis management, comms, etc.)
4. Are our **backups** on separate networks from our production systems? Have we tested that our **backups are not accessible** by a potential attacker?
5. When was the last time we performed **full backup restoration tests** of our systems? What were the results?
6. How long would it take to **recover** from a widespread cyberattack? In what order would we **restore** our systems if everything were down?
7. How much **cyber insurance coverage** do we have? What does it cover and not cover? Are there any special requirements we need to meet for coverage to be in force?
8. Are we testing our workforce with **phishing tests**? What have been the results this past year?
9. Are we using **multi-factor authentication (MFA)**? Are there systems where we are not using MFA and why? How are we systematically controlling privileged accounts (e.g. admin and system accounts).
10. Do we have a full list of direct and indirect **third-party vendors**? Do we know which ones are most risky from a cyber standpoint and do we have the right mitigations in place?

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]

Emerging trends in corporate cybersecurity governance

Cybersecurity Committee/ Sub-Committee

Industry CISO Advisory Board

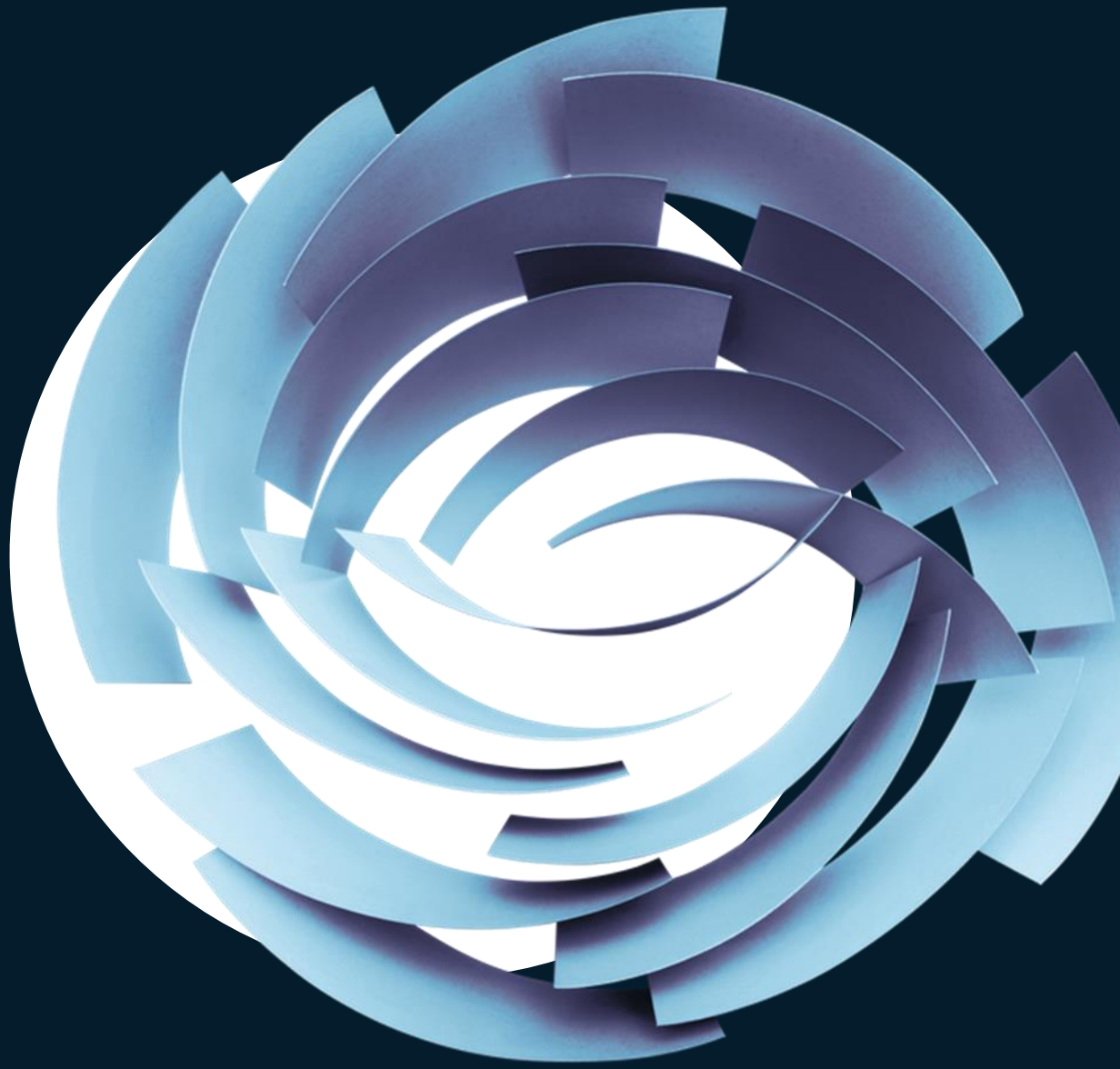
Agenda

Why does cybersecurity matter?

How do boards engage with cybersecurity?

What does effective cybersecurity look like?

Q&A



The NIST cybersecurity framework is a set of guidelines used to assess and manage cybersecurity risks through five key functions

Cyber-security functions	Identify	Protect	Detect	Respond	Recover
Description	Development of an organizational understanding to managing cybersecurity risk	Appropriate safeguards to ensure delivery of critical infrastructure services	Activities to identify the occurrence of a cybersecurity event	Activities to take action regarding a detected cybersecurity incident	Activities to maintain plans for resilience and restore any impaired capabilities/ services incident.
Sample Activities	Identify top assets Understand top risks	Secure data Protect network entry points Control access rights	Monitor for unusual network activity Detect unusual behavior	Mitigate the attack Communicate with stakeholders on the incident	Restore business services Conduct postmortems Integrate learnings

While NIST CSF provides a framework, security organizations bring it to life through capabilities

1. Strategy, Program Management, & 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

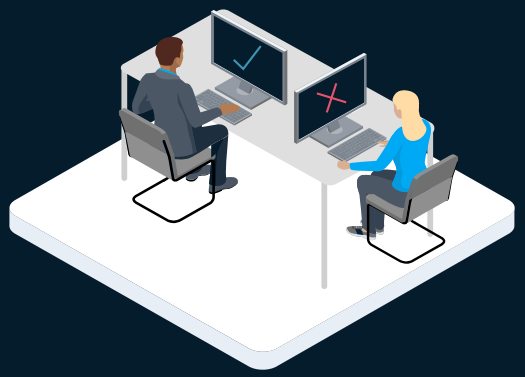
Each cyber capability has a set of sub-capabilities
(1 of 2)

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



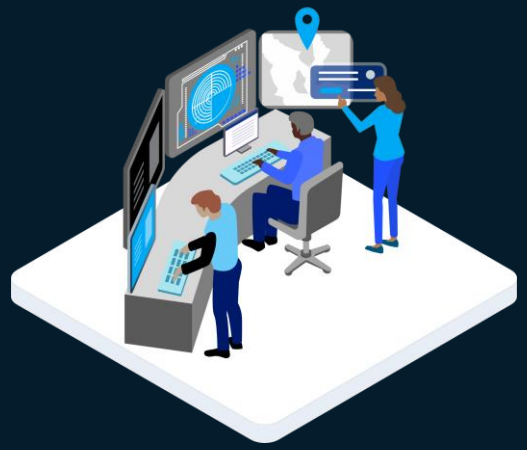
3 Identity and Access Management

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	

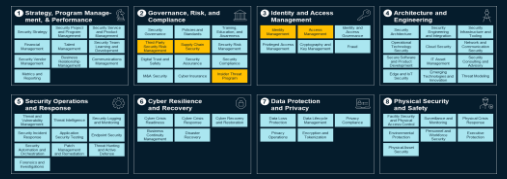
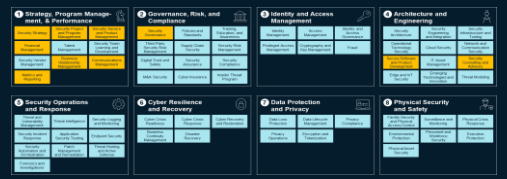
7 Data Protection and Privacy

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

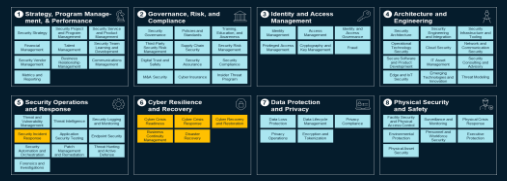
8 Physical Security and Safety

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

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

Summary and key takeaways

Summary

Organizations continue to modernize and transform their business models into digital enterprises

While digital transformation presents unparalleled opportunities for growth, it also increases the attack surface for cyber criminal exploitation, causing widespread damage and disruption

Cyber attacks and threat actors continue to become more sophisticated and have evolved from “opportunists” to well-funded, highly organized, and well-trained cyber criminals, often backed by nation-states for geo-political gain

Companies have traditionally struggled to invest at-pace with the rising threat and have thus taken a reactive approach to protecting business operations

Planning and preparation is paramount. To create proactive cybersecurity, organizations must embed cybersecurity into all business functions by-design, creating a secure and trusted foundation rather than bolting it on after the fact

We believe effective cybersecurity creates a competitive differentiator that, when considered up-front, allows organizations accelerate their mission and protect their purpose

Key takeaways

- Cybersecurity is a strategic business risk that has the potential to disrupt but it can also be a competitive advantage when done right
- Cybersecurity threats will continue to increase in volume and sophistication, so a well-designed, well-managed, and adequately-funded cybersecurity program is vital
- Boards play a key role in overseeing cyber programs and the expectations for their involvement and knowledge about cybersecurity is increasing
- Effective cybersecurity is composed of “layers of defenses,” but its remit varies from company to company
- There are key steps organizations can take to futureproof themselves against the threats of tomorrow

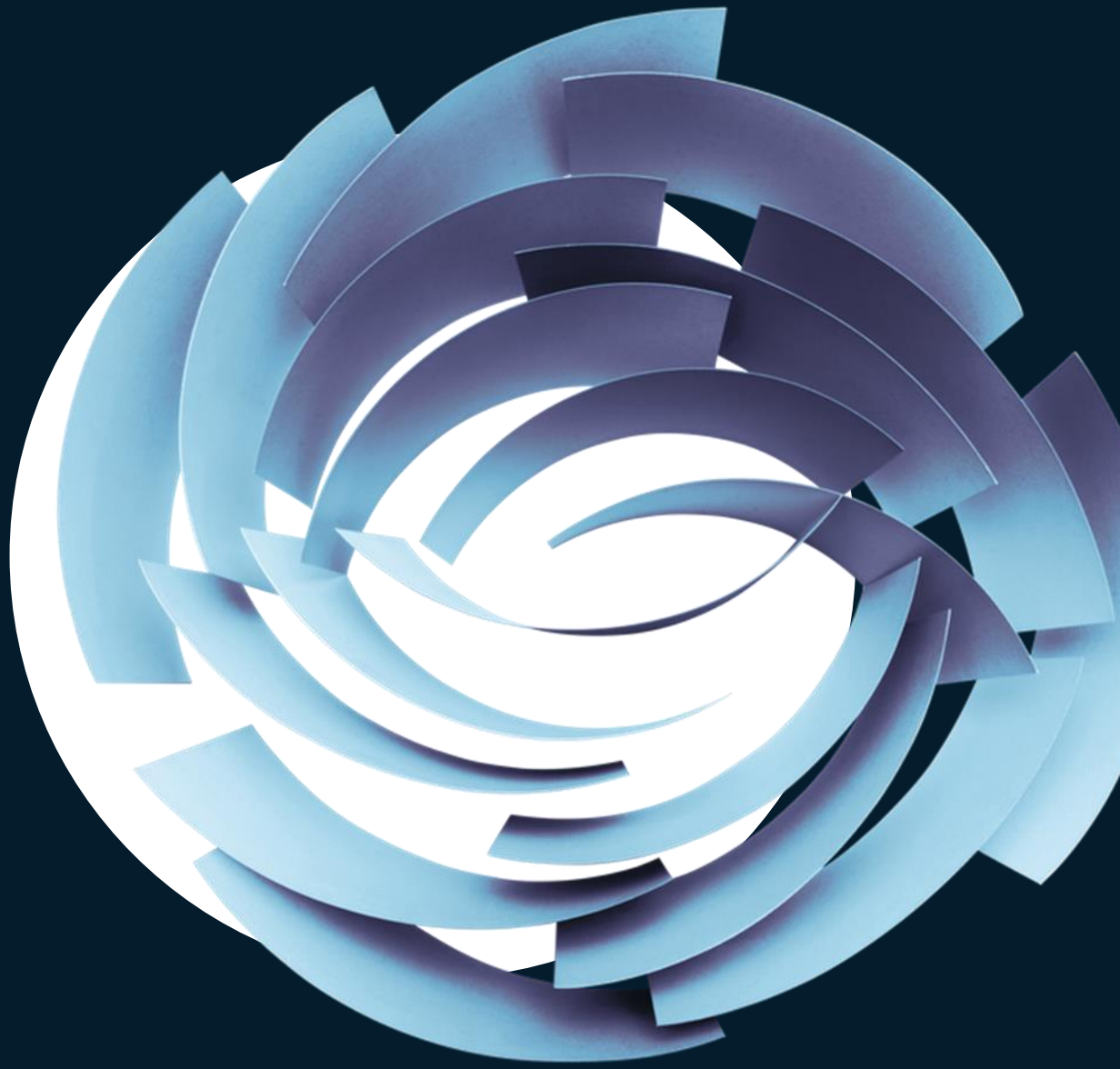
Agenda

Why does cybersecurity matter?

How do boards engage with cybersecurity?

What does effective cybersecurity look like?

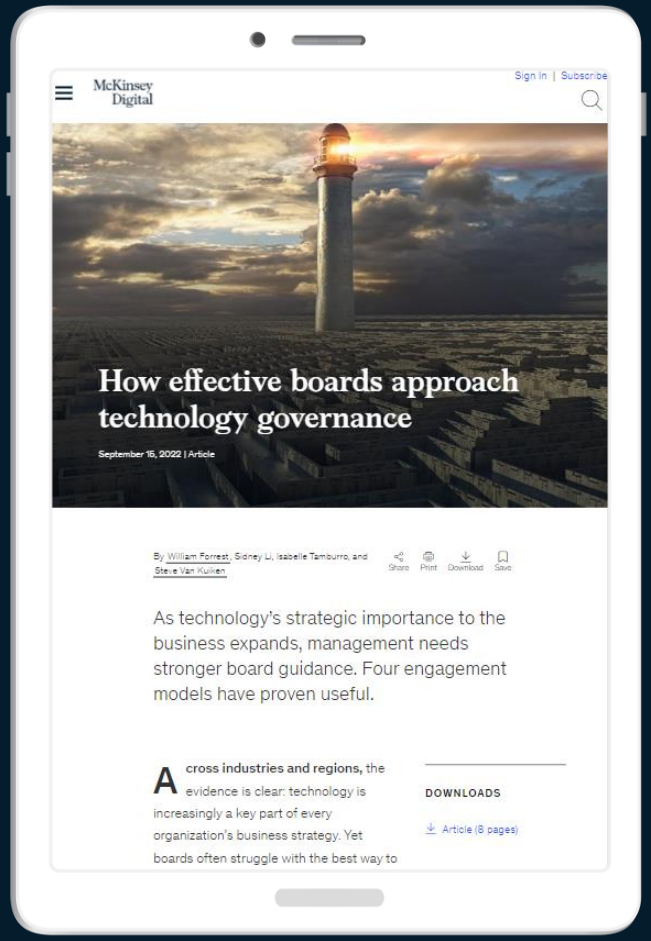
Q&A



Q&A

Aditional Reading: “How effective boards approach technology governance”

Published September 22, 2022 on McKinsey.com



“As technology’s strategic importance to the business expands, management needs stronger board guidance. Four engagement models have proven useful.”

Four effective models through which boards engage with management on technology issues:

1. Regular, full-board engagement as a recurring agenda item
2. Formal, standing technology committees
3. Temporary and/or advisory tech committees
4. Informal engagement on select topics

Article Link
https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/how-effective-boards-approach-technology-governance

Thank you

Justin Greis

Partner, Chicago

Justin_Greis@mckinsey.com

linkedin.com/in/justingreis

Twitter: @JustinGreis

Brian Kelly

Senior Advisor, Wilmington

linkedin.com/in/brian-kelly-b623224/