

# The Future of Cybersecurity

Institute for Corporate Governance (ICG)  
Kelley School of Business, Indiana University

May 2022

Justin Greis, Partner

Jeff Caso, Associate Partner

Charlie Lewis, Associate Partner

CONFIDENTIAL AND PROPRIETARY

Any use of this material without specific permission of McKinsey & Company  
is strictly prohibited

# We will look at the future of cybersecurity in three different ways

---



## **The cybersecurity market today**

How the cybersecurity provider market is addressing future challenges



## **Digital and technology trends of tomorrow**

Technology forces that will impact our world tomorrow and what it means today



## **Futureproofing cybersecurity**

Transformational recipes that can ready organizations to tackle future cybersecurity challenges



# Introductions

## Our knowledge is rooted in serving clients

# 500+

Cybersecurity engagements with over 50 cyber transformations in the last 4 years

# 50+

Cybersecurity software, hardware, and services providers and investors served in 2020-2021

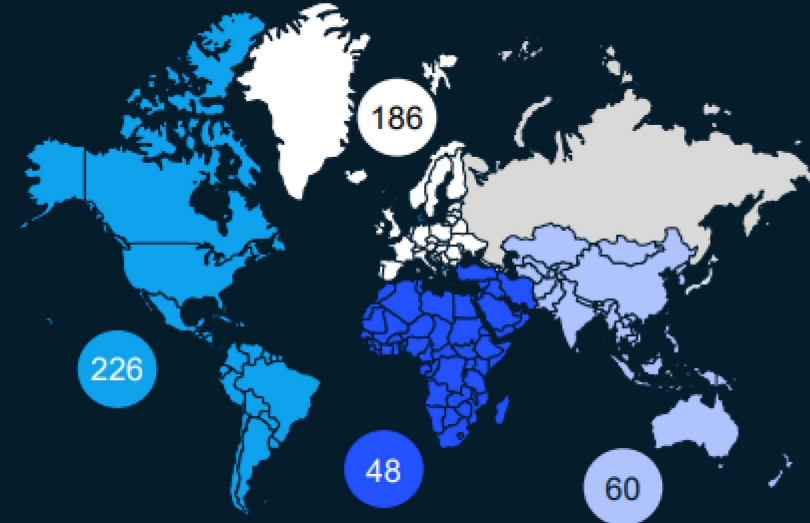
# 100+

**CISOs engaged in industry roundtables on quarterly basis**

Industry-specific CISO round-tables with focus on healthcare, insurance, and financial services.

**Engaged several boards and industry forums** to define cyber strategy for global organizations

## Spread across the globe



## Today's speakers



**Justin Greis**  
Partner  
Chicago



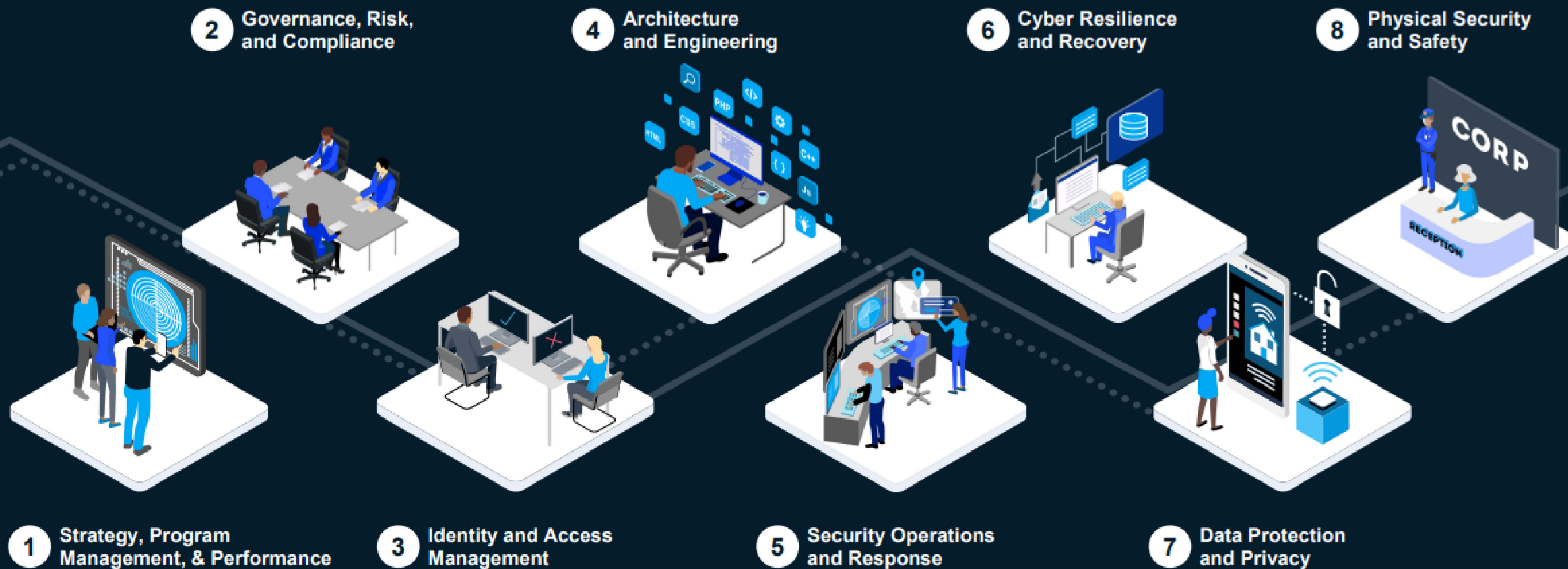
**Charlie Lewis**  
Associate Partner  
Stamford



**Jeffrey Caso**  
Associate Partner  
Washington D.C.

*Coauthors and key contributors: Anselm Ohme, Daniel Wallance, David Hall, Hannah Chen, Jim Boehm, Joe Revier, Kathleen Li, and Peter Russell*

# Defining Cybersecurity







## 1. The Cybersecurity Market

## 2. Digital and Technology Trends

## 3. Futureproofing Cybersecurity

---

## Poll question #1

I believe cybersecurity is a critical business capability - on par with other business functions (e.g. finance, marketing, sales, etc.) - for companies today.

---

- 
- A Strongly agree
  - B Agree
  - C Neither agree nor disagree
  - D Disagree
  - E Strongly disagree
-

# Six key trends shaping near-term cybersecurity market

---



**1**

**Growth of hybrid and multi-cloud**



**2**

**Increased acceptance of  
Software as a Service (SaaS)  
cyber**



**3**

**Regulatory pressure  
and splinternet**



**4**

**Automation and DevOps**



**5**

**Shift from Protect to Detect and  
Respond**



**6**

**Market consolidation**

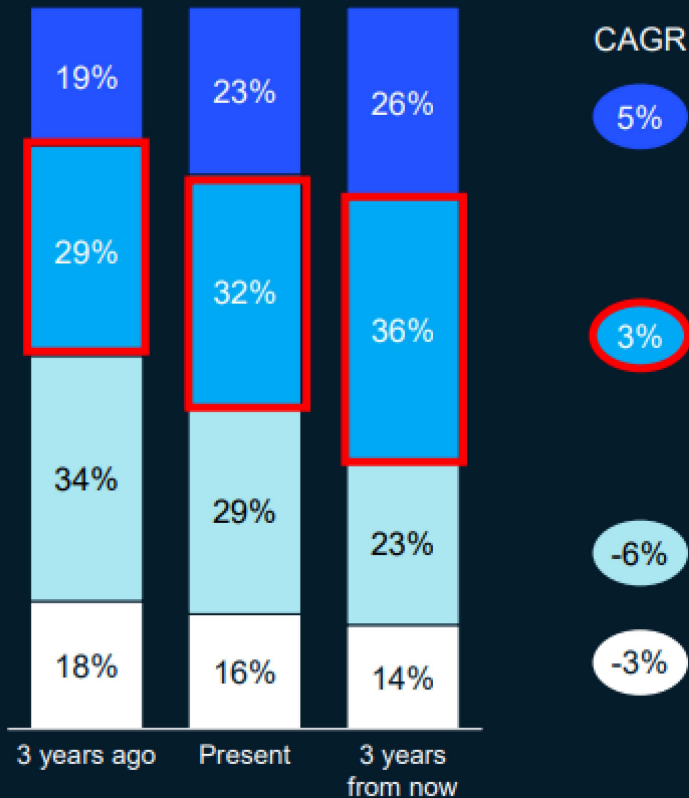


# 1. Public cloud migration expected to progress at 3-4x the rate in highly regulated industries vs. less regulated industries

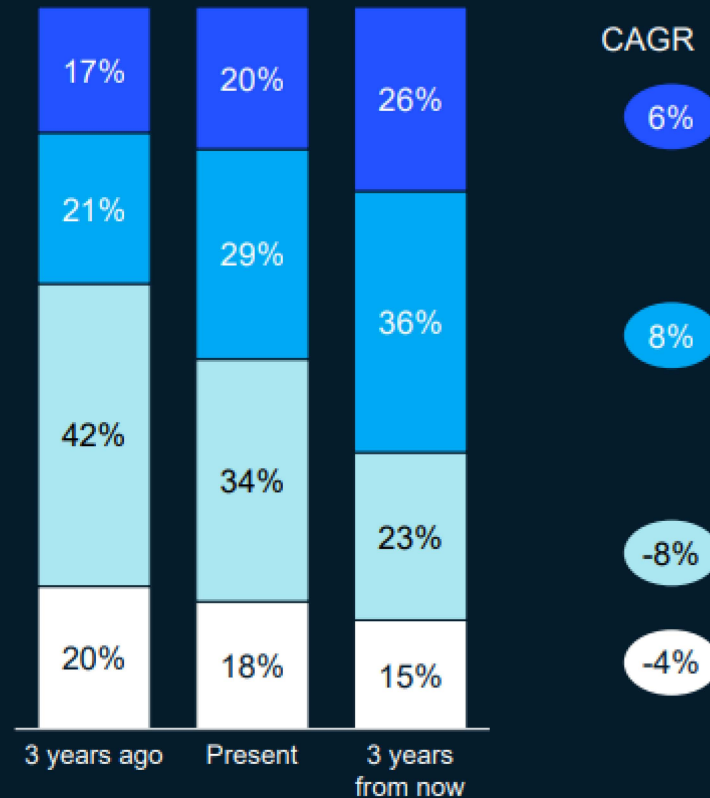
## Infrastructure distribution by regulated industry

Private cloud Public cloud Corporate data centers Co-located/managed

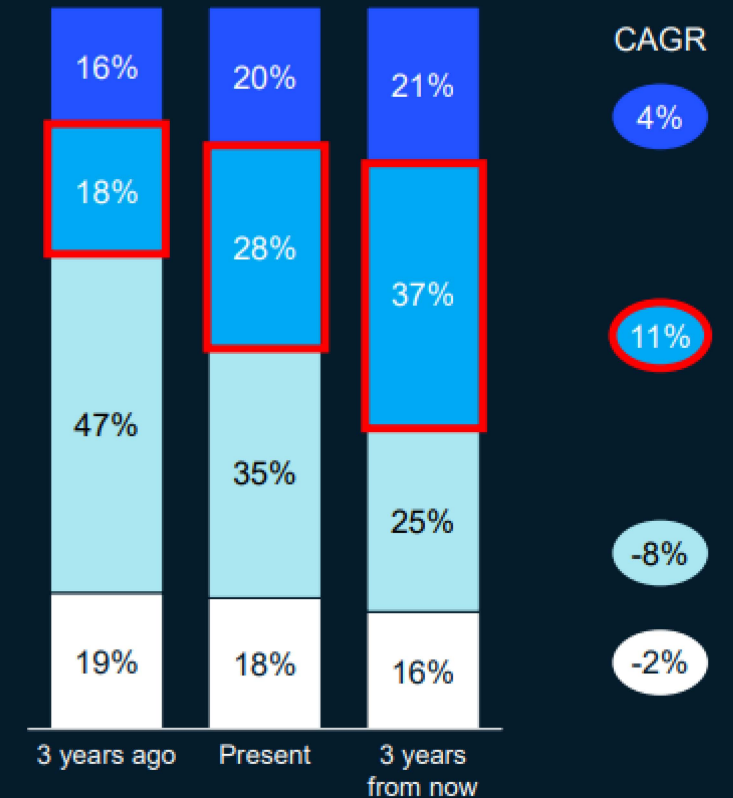
### Less regulated



### Moderately regulated



### Highly regulated



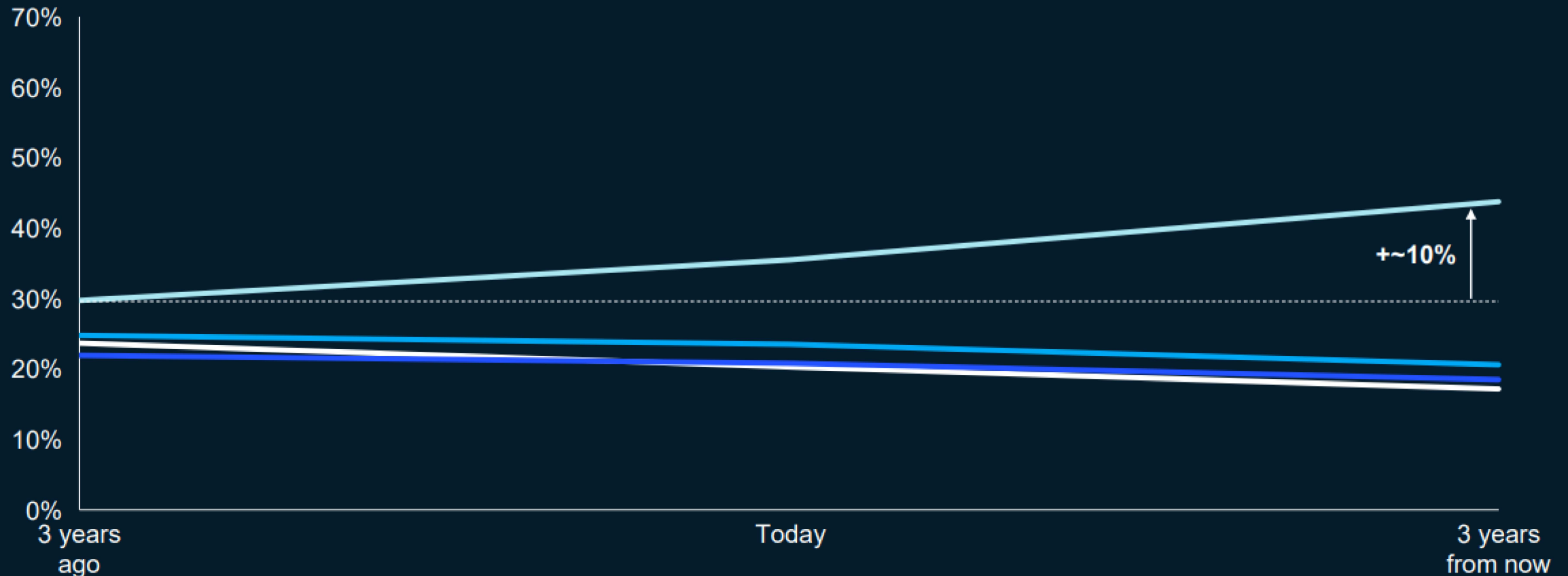
Note: High regulation – banking, insurance, government; Medium regulation – consumer/retail, utilities, transportation, telecommunications, healthcare; Low regulation – manufacturing, software, media, education



## 2. Usage of SaaS cybersecurity solutions are anticipated to accelerate by 10%+ p.p. over the next 3 years

— Hardware — Software (appliance-based) — Software (agent-based) — SaaS

Aggregate product types over time across eleven<sup>1</sup> cybersecurity market segments (n=462)



1. MSSP and security consulting omitted due to service-based models



### 3. Recent and anticipated regulatory changes may compel companies to revisit their data privacy strategy

■ Some data protection / localization laws in place    ■ No information / no data protection laws in place

>75% of countries have data protection laws...



...with which organizations must keep pace.

**Organizations may require new tools and data management practices** that facilitate local data storage and processing, chart data lineage, and manage data processing workflows

**Consider new guard-rails.** Many software/solution providers refrain from operating in certain countries or sectors where the addressable market is outweighed by digital compliance costs;

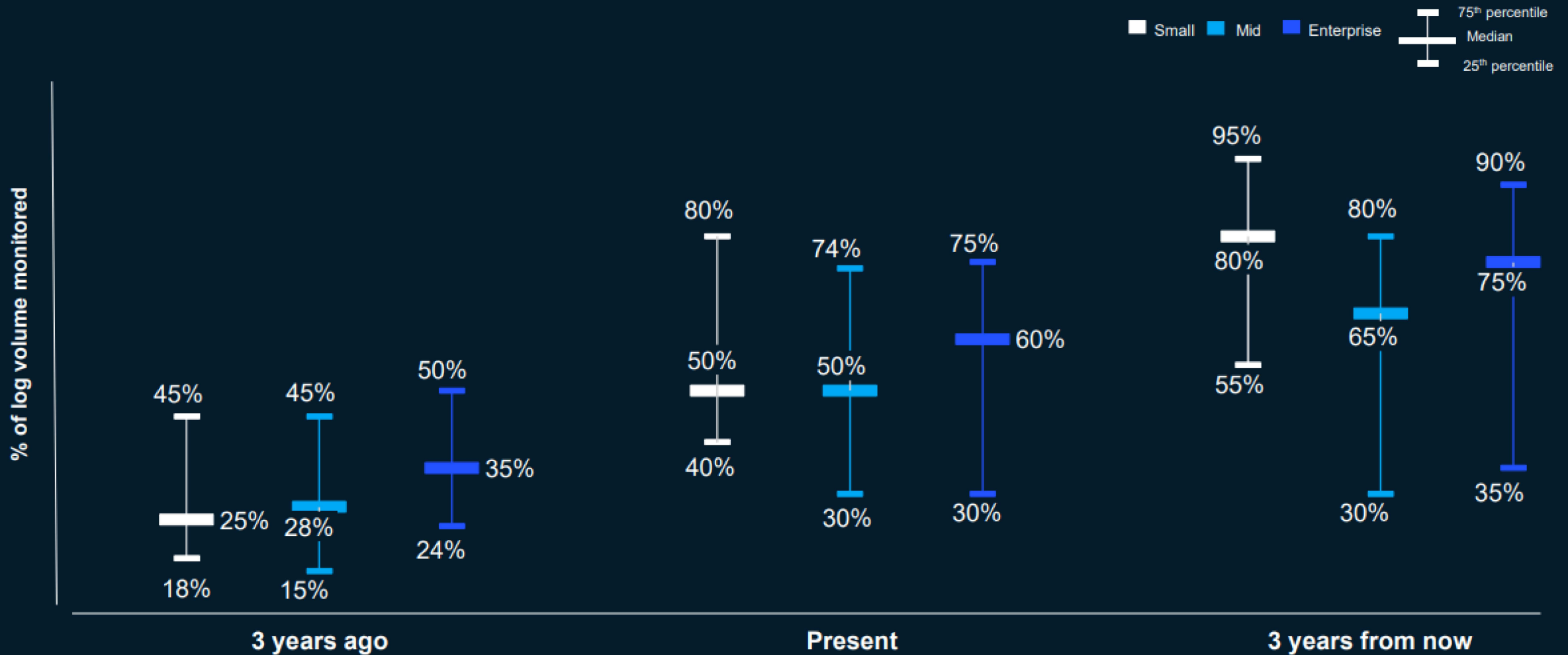
**Organizations may require training** to identify data handling and localization risks across customer and internal data / processes (e.g., model development, cloud instance deployment)

1. Individual countries and regions should be evaluated and prioritized based on their relative importance to the organization





## 4. Enterprise Security Operations Center visibility expected to increase to ~75% total log volume in 3 years vs. ~35% 3 years ago

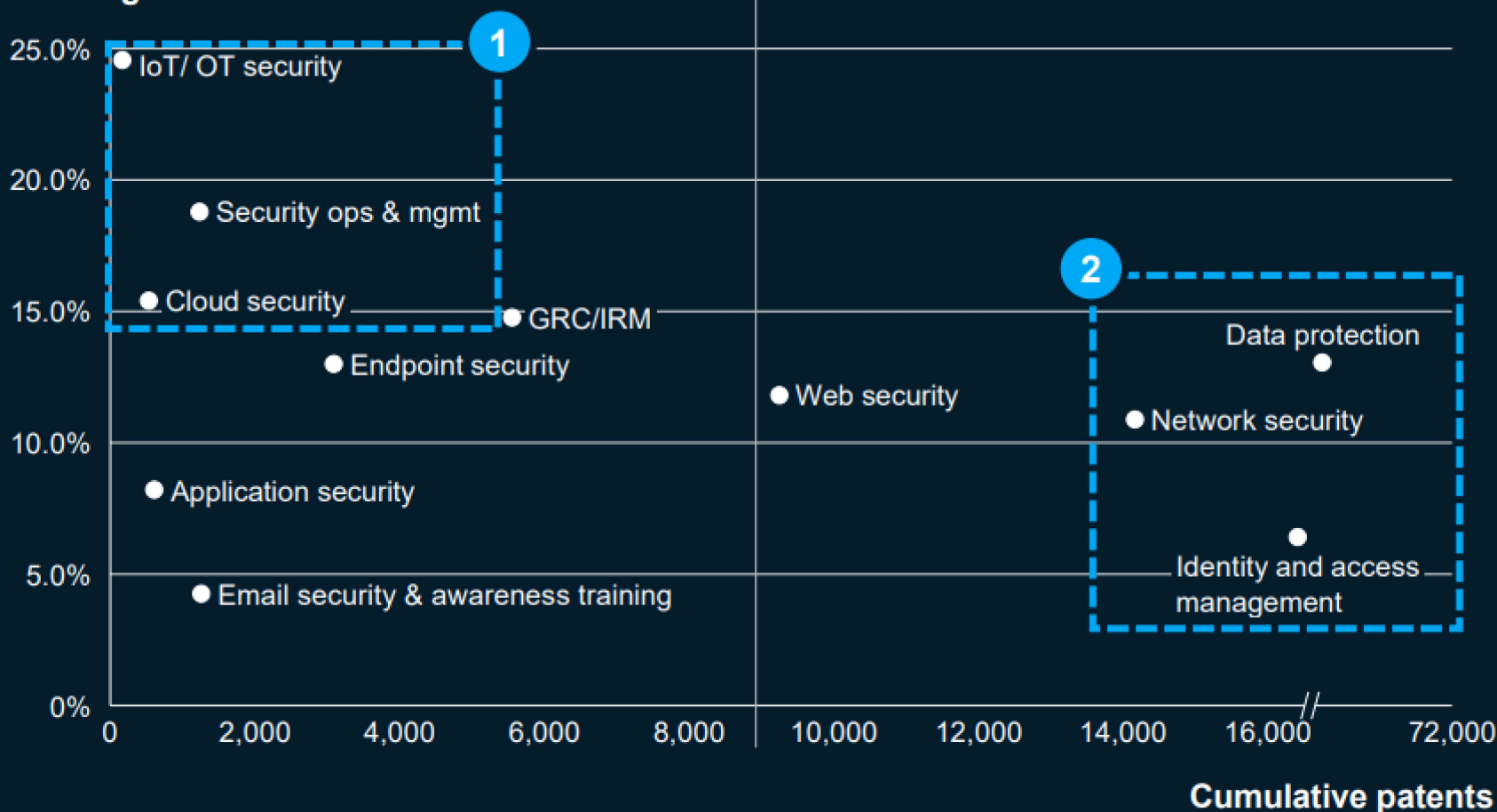




## 5. Expanding attack surface area (e.g., OT, cloud) is driving key innovation in cybersecurity

Patents granted globally, 2017-2021

### Patent growth CAGR



**1** IOT/OT, security operations and management, and cloud security are rapidly increasing the speed of technology innovation

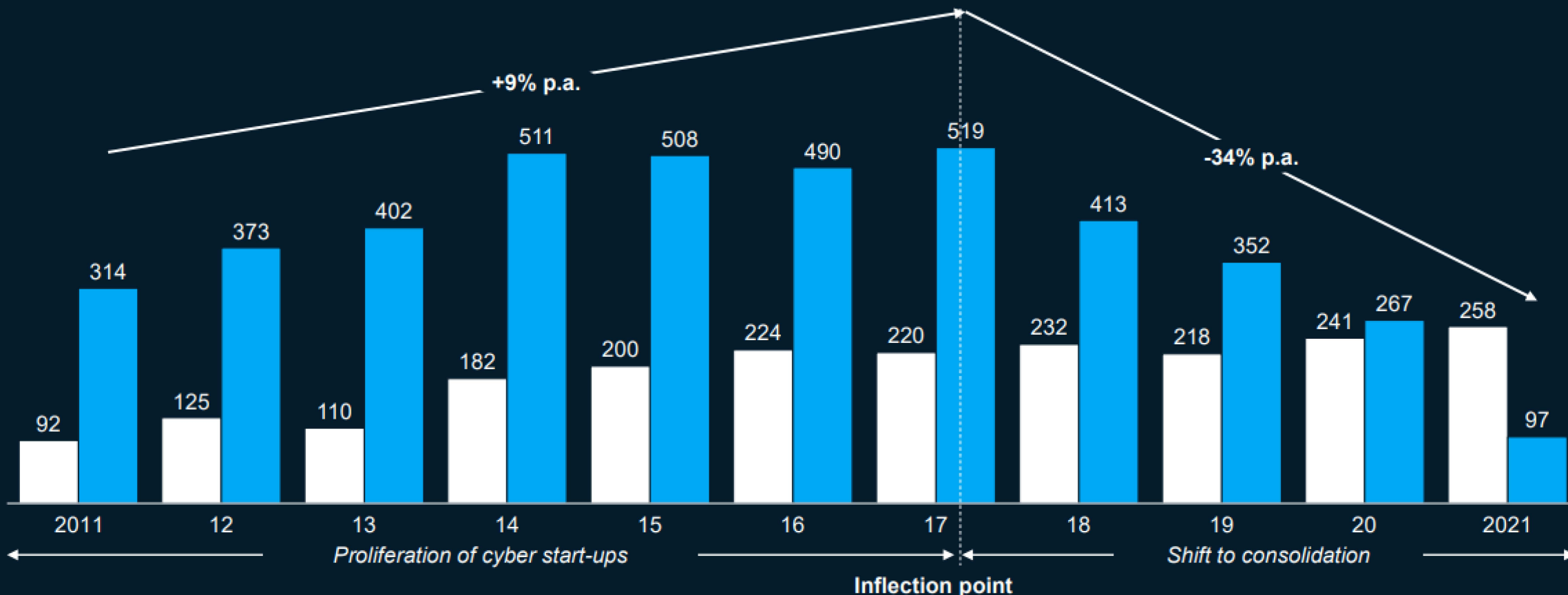
**2** Mature cybersecurity segments have slowed (e.g., data protection, network and identity) in terms of patent growth as they reach innovation saturation



## 6. The market may have reached a “post-peak” trough in new company formation while consolidation is rising

■ # of M&A deals ■ # of new cybersecurity companies formed

M&A deals versus new cybersecurity companies formed – CAGR indicates change in new company formation





# Takeaways

---



**1**

## **Growth of hybrid and multi-cloud**

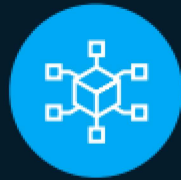
Multi-cloud and hybrid environments are increasing in complexity, with a purely “cloud-native” world still far off



**2**

## **Increased acceptance of SaaS cyber**

Usage of SaaS cybersecurity solutions is anticipated to accelerate by 10%+ over the coming 3 years



**3**

## **Regulatory pressure and splinternet**

Countries are developing data privacy, protection and localization regulations to which companies must adapt



**4**

## **Automation and DevOps**

Digitization is expanding log volumes which requires capacity and automation, while agile developers face increased security responsibilities



**5**

## **Shift from Protect to Detect and Respond**

A growing number of attack surfaces (e.g., IoT devices) and attackers is increasing the remit of the security organization



**6**

## **Cyber market is consolidating**

Cybersecurity market may have reached a “post-peak” trough in new company formation – # of new cyber companies formed slowing down while M&A deals are on a rise



1. The Cybersecurity Market

**2. Digital and Technology Trends**

3. Futureproofing Cybersecurity

---

## Poll question #2

I believe companies are taking the appropriate steps to ensure the security and privacy of the data they store (e.g. consumer data, financial data, confidential internal data).

---

- 
- A Strongly agree
  - B Agree
  - C Neither agree nor disagree
  - D Disagree
  - E Strongly disagree
-

# We attempted to look into the future of cybersecurity in 10-15 years

## Digital trends

What are the top digital trends that will impact business and global economy between now and 2050?

## Technology enablers

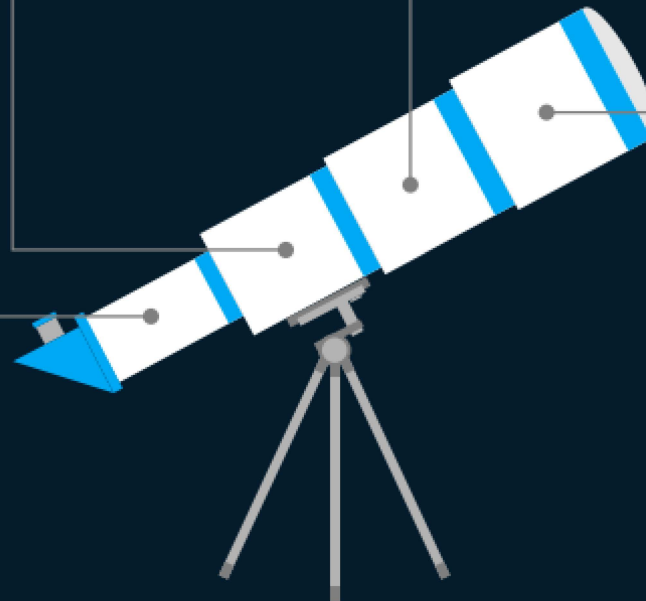
Underpinning those digital trends, what technology enablers are required to build those capabilities?

## Cyber implications

What are the cybersecurity implications of those technology enablers that cybersecurity organizations will have to contend with?

## Future scenarios

Between now and the next 10 years, what are the disruptive scenarios by which these digital trends could evolve? What is the resulting impact on the future of cybersecurity?





# In the next 10-15 years, technology will continue to disrupt global business

Effects of technology trends up to 2050



**50%**



of today's work activities could be automated by 2025

**~30x**



reduction in the working time required for software development and analytics

**>75%**



of enterprise-generated data will be processed by edge or cloud computing by 2025

**~10%**



of global GDP could be associated with blockchain by 2027

**Up to 80%**



of global population could be reached by 5G coverage by 2030

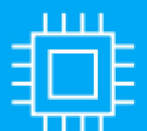
**>75%**



of all digital-service touch points (e.g., voice assistants) will see improved usability, enriched personalization, and increased conversion

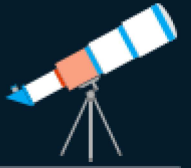
value potential of quantum-computing use cases at full scale by 2035

**>\$1 trillion**



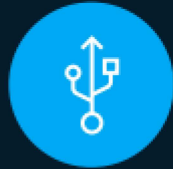
# A recent McKinsey initiative identified several “digital trends” likely to have disproportionate impact across industries

Technologies underpinning these digital trends



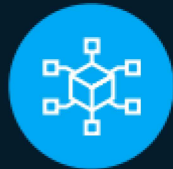
## 1 Next-level process automation and virtualization

- 1a. AR / VR workspaces
- 1b. Nanobot-enabled manufacturing
- 1c. Dynamic supply chains



## 2 Future of connectivity

- 2a. 5G-enabled digital ecosystems
- 2b. “Branch-of-the-future”
- 2c. Developing market technologization



## 3 Distributed infrastructure

- 3a. XaaS proliferation
- 3b. Cloud / edge
- 3c. Infra-as-code



## 4 Next-generation computing

- 4a. Quantum computing
- 4b. Identity-as-code
- 4c. Bottomless data lakes



## 5 Applied AI

- 5a. Fully autonomous vehicles
- 5b. Smart cities
- 5c. Deep learning



## 6 Future of programming

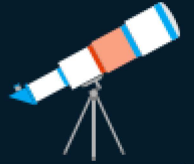
- 6a. Low-code / no-code solutions
- 6b. Self-healing code
- 6c. Open-source by default



## 7 Trust architecture

- 7a. Crypto / blockchain
- 7b. Self-sovereign identity
- 7c. Passwordless authentication

# Each technology enabler has associated cybersecurity challenges – our research reveals 11 primary challenges



Technologies underpinning these digital trends

## Technology enablers

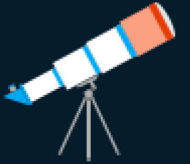


## Cybersecurity challenges





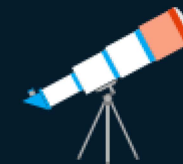
# If these “sticky” cybersecurity challenges are not addressed, what could the future look like?



| Unsolved challenge                                                                                                                                                                   | Scenario                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| A. Mass proliferation of alternate identities (e.g., machine, bot, AR / VR)                                                                                                          |  <b>Universal identity fraud</b>          |
| B. Dramatic expansion of attack surface area (e.g., multi-multi-cloud, day-to-day changes)                                                                                           |  <b>Mass network rebuild</b>              |
| C. Supplier risk “fog” (i.e. as a result of dynamic supply chain)                                                                                                                    |  <b>Multi-supply chains</b>               |
| D. Limitations to enterprise “omnipotence” in policy control (i.e. due to mass XaaS outsourcing)                                                                                     |  <b>Existential challenge to CISO org</b> |
| E. Untraceable asset management (i.e. asset management / hosting does not resolve)                                                                                                   |  <b>Asset sprawl</b>                      |
| F. Degraded confidence interval on identity verification (i.e. as a result of crypto / blockchain)                                                                                   |  <b>Ubiquitous biometrics</b>             |
| G. Challenges to existing encryption methodologies (i.e. need for quantum-secure encryption)                                                                                         |  <b>Quantum revolution</b>                |
| H. Splintering between business, IT, and OT digital teams (i.e. as a result of shop floor digitization or business use of LC/NC platforms) forces new approaches to cyber governance |  <b>Cyber militarization</b>             |
| I. Off-network security (i.e. in autonomous vehicles) requires offline security engine                                                                                               |  <b>Splinternet</b>                     |
| J. Consumer security challenges                                                                                                                                                      |  <b>Digital pandemic</b>                |
| K. Increase in size of models limits ability to validate data integrity                                                                                                              |  <b>Algorithmic distrust</b>            |



# Takeaway: bringing it all together...



In order to plan for a digital future...

...there are a series of cybersecurity scenarios that need to be futureproofed

Next-level process automation and virtualization

Next-generation computing

Trust architecture

Future of connectivity

Applied AI

Distributed infrastructure

Future of programming



Universal identity fraud



Mass network rebuild



Multi-supply chains



Existential challenge to CISO org



Asset sprawl



Ubiquitous biometrics



Cyber militarization



Splinternet



Digital pandemic



Quantum revolution



Algorithmic distrust



1. The Cybersecurity Market

2. Digital and Technology Trends

**3. Futureproofing Cybersecurity**

---

## Poll question #3

I believe cyber-defenders are  
\_\_\_\_\_ attackers

---

- 
- A Far ahead of
  - B Reasonably outpacing
  - C Keeping up with
  - D Falling behind
  - E Way behind
-



# Recall: the eight core security capabilities



# Each security capability has a set of sub-capabilities (1/2)



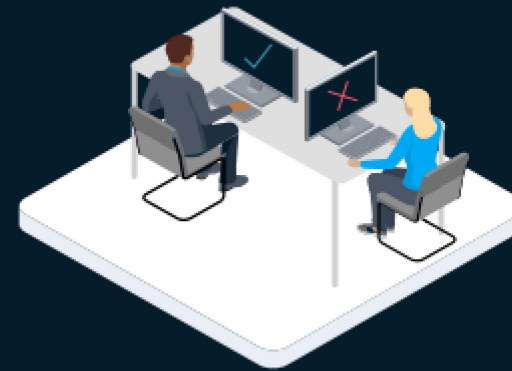
## 1 Strategy, Program Management, & Performance

|                            |                                         |                                         |
|----------------------------|-----------------------------------------|-----------------------------------------|
| 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 security capability has a set of sub-capabilities (2/2)



## 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 |                    |

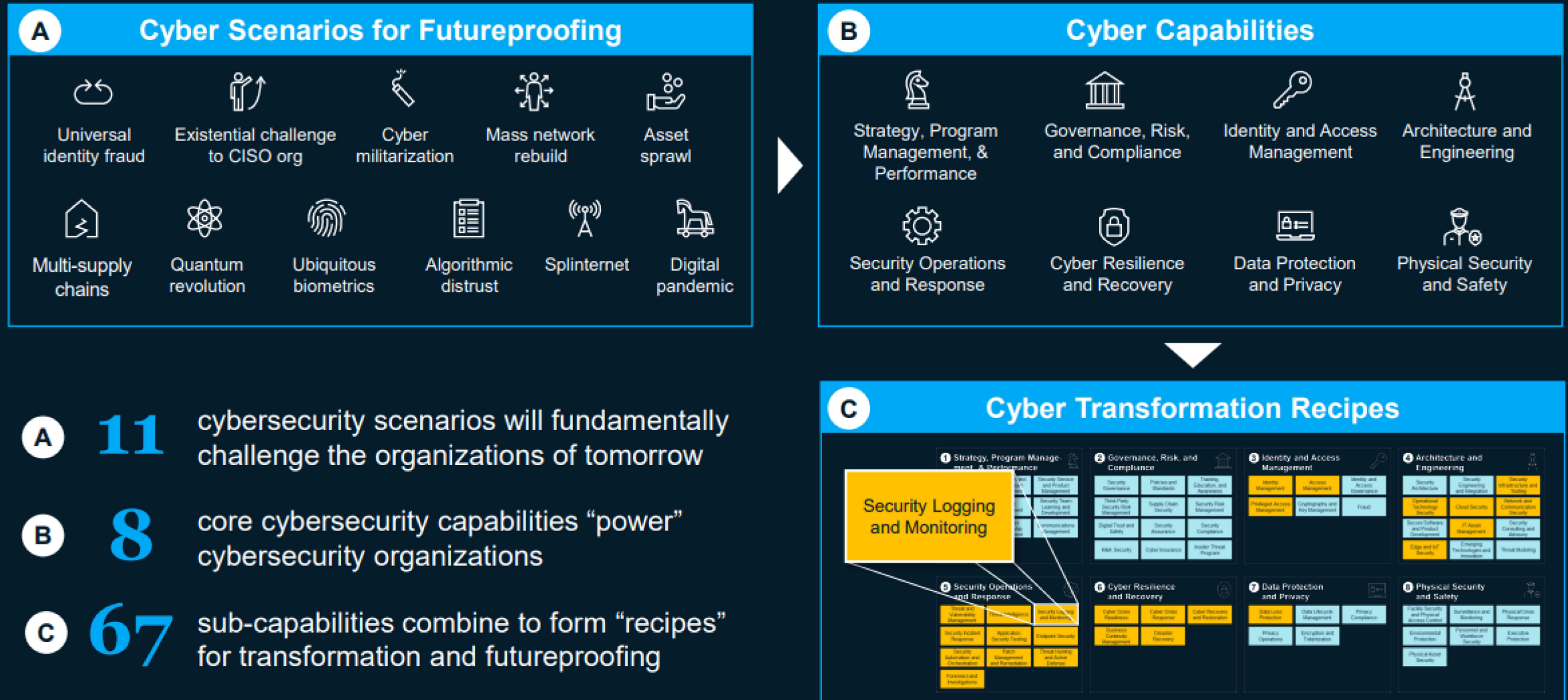


## 8 Physical Security and Safety

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



# Transforming combinations of cybersecurity capabilities today can help futureproof against the scenarios of tomorrow



# Cybersecurity futureproofing recipes (1 of 2)

| Cyber transformation recipe                                                                    | Impacted capabilities                                                                 | Top 3 steps to take today                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. <b>Invest</b> in talent and empower your leaders                                            |    | <ul style="list-style-type: none"> <li>• <b>Leadership development programs</b></li> <li>• Invest in strong cyber recruiting pipelines</li> <li>• Deploy technical upskilling/education program</li> </ul>                 |
| 2. <b>Know</b> your users and your n <sup>th</sup> party ecosystem                             |    | <ul style="list-style-type: none"> <li>• <b>Invest in strong IAM capabilities</b></li> <li>• <b>Inventory and risk-assess all third-parties</b></li> <li>• Assess supply chain security and build resilience</li> </ul>    |
| 3. <b>Defend</b> your assets and your data                                                     |    | <ul style="list-style-type: none"> <li>• <b>Inventory your crown jewel assets and data</b></li> <li>• Understand the privacy-related regulations</li> <li>• Implement strong encryption over sensitive data</li> </ul>     |
| 4. <b>Build</b> trust by design (security, privacy, and compliance) into products and services |   | <ul style="list-style-type: none"> <li>• <b>Develop strong DevSecPrivOps processes</b></li> <li>• Create real-time compliance monitoring</li> <li>• Train and empower development/product teams</li> </ul>                 |
| 5. <b>Embed</b> deep within the business and products and services                             |  | <ul style="list-style-type: none"> <li>• <b>Deploy BISOs &amp; security champion program</b></li> <li>• Measure/improve engagement and satisfaction</li> <li>• Build service-oriented, platform-enabled catalog</li> </ul> |



# Cybersecurity futureproofing recipes (2 of 2)

| Cyber transformation recipe                                              | Impacted capabilities                                                                 | Top 3 steps to take today                                                                                                                                                                                                         |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6. <b>Listen</b> to your environment and prepare to respond              |    | <ul style="list-style-type: none"> <li>• <b>Ensure completeness &amp; depth of monitoring</b></li> <li>• Create and exercise incident response playbook</li> <li>• Assess technical readiness/response capabilities</li> </ul>    |
| 7. <b>Plan</b> for disruption and practice “from scratch” recovery       |    | <ul style="list-style-type: none"> <li>• <b>Perform cyber crisis simulations/wargames</b></li> <li>• Build cyber crisis management program</li> <li>• Build extreme recovery/restoration capabilities</li> </ul>                  |
| 8. <b>Measure</b> , synthesize, and communicate in business terms        |    | <ul style="list-style-type: none"> <li>• <b>Build business-oriented board reporting</b></li> <li>• Define the cyber metrics that matter</li> <li>• Educate board and provide ongoing updates</li> </ul>                           |
| 9. <b>Converge</b> enterprise, product, OT, and physical security        |   | <ul style="list-style-type: none"> <li>• <b>Assess OT assets &amp; extend cyber controls</b></li> <li>• Integrate physical and cybersecurity monitoring</li> <li>• Extend security controls to customer products</li> </ul>       |
| 10. <b>Adopt</b> a cloud-first mindset and experiment with emerging tech |  | <ul style="list-style-type: none"> <li>• <b>Build secure cloud landing zones &amp; controls</b></li> <li>• Integrate cloud security into IT/Business/products</li> <li>• Reward and recognize innovation with new tech</li> </ul> |



# 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 to 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



---

## Poll question #4

I believe most cybersecurity organizations today are taking the right steps to overcome future digital challenges.

- ☐ A Strongly agree
- ☐ B Agree
- ☐ C Neither agree nor disagree
- ☐ D Disagree
- ☐ E Strongly disagree



# Q&A



# Thank you



## Justin Greis

Partner | Chicago

[Justin\\_Greis@mckinsey.com](mailto:Justin_Greis@mckinsey.com)

[linkedin.com/in/justingreis](https://www.linkedin.com/in/justingreis)

Twitter: @JustinGreis



## Charlie Lewis

Associate Partner | Stamford

[Charlie\\_Lewis@mckinsey.com](mailto:Charlie_Lewis@mckinsey.com)

[linkedin.com/in/charlesdavidlewis](https://www.linkedin.com/in/charlesdavidlewis)



## Jeffrey Caso

Associate Partner | Washington D.C.

[Jeffrey\\_Caso@mckinsey.com](mailto:Jeffrey_Caso@mckinsey.com)

[linkedin.com/in/jeffrey-caso-95112a41](https://www.linkedin.com/in/jeffrey-caso-95112a41)