# Investing in cybersecurity: building resilient cybersecurity programs and portfolios

## Information Security Forum (ISF) North America Conference 2021

ForgePoint CAPITAL

EY
Building a better working world

# About today's speakers

## Justin Greis

- Partner, EY
- Chicago, Illinois
- Global and Americas Cybersecurity Strategy, Risk, Compliance, and Resilience Leader

justin.greis@ey.com

linkedin.com/in/justingreis

justingreis.com

@JustinGreis

## Will Lin

- Managing Director and Founding Member, ForgePoint Capital
- San Francisco, California
- Board member for several cybersecurity companies

wlin@forgepointcap.com

linkedin.com/in/linwilliam/

forgepointcap.com

@WilliamLin

# Agenda

1. Today's security landscape
2. 5 common themes in security program assessments
3. Making sense of the vendor ecosystem and cyber start-ups
4. Questions and answers

ForgePoint CAPITAL

EY

# 1

# Today's security landscape

# Polling question 1

How would you describe the volume of cyber incidents in your organization (or clients' organizations) this past year?

A Increased dramatically

B Increased slightly

C Relatively unchanged

D Decreased slightly

E Decreased dramatically

# Polling question 2

Rank the threat actors that you have encountered this past year from most frequent to least frequent. (5 = most frequent; 1 = least frequent)

A Third-parties (e.g. vendors, partners, and suppliers)

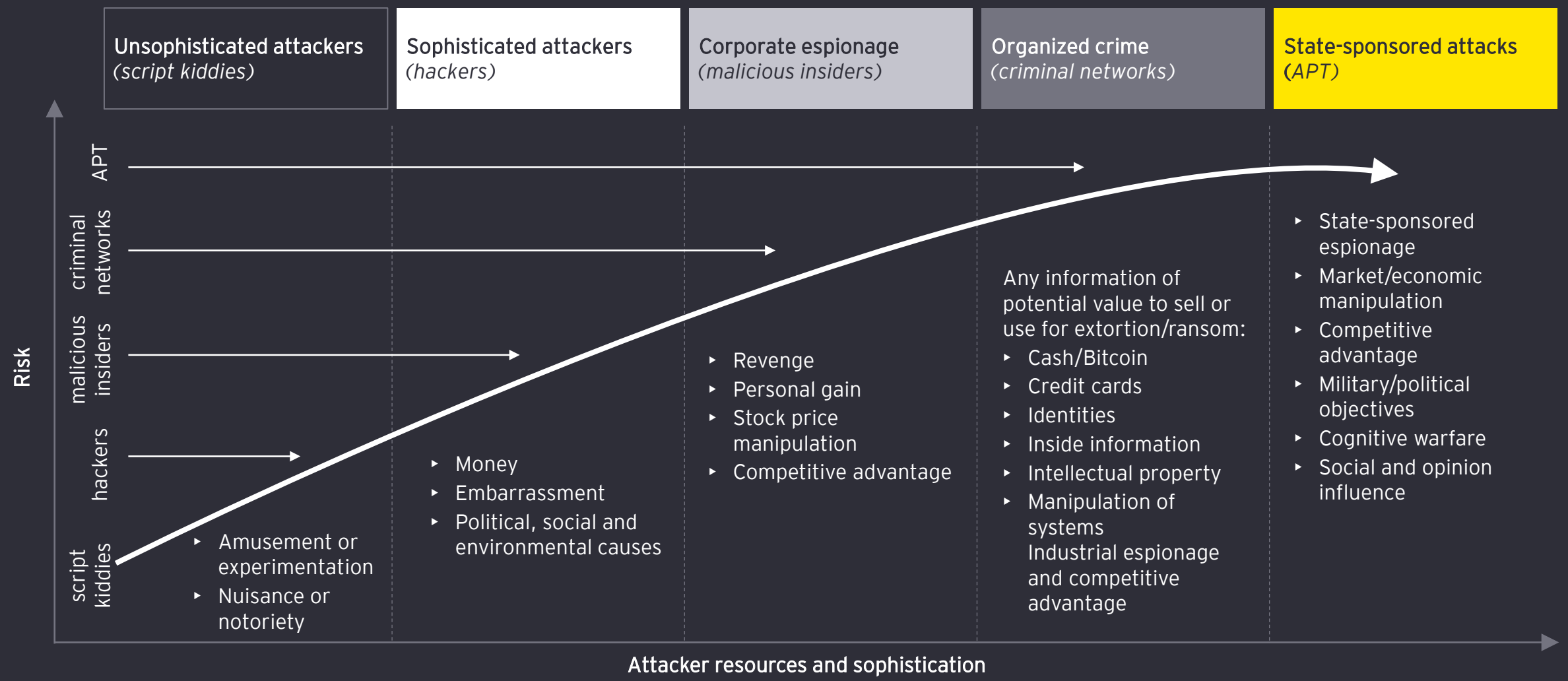
B Malicious insiders (e.g. employees)

C Hacktivists groups, politically motivated hackers, or "attention-getters"

D Cyber criminal rings/organized crime (e.g. ransomware groups)

E Nation-state actors

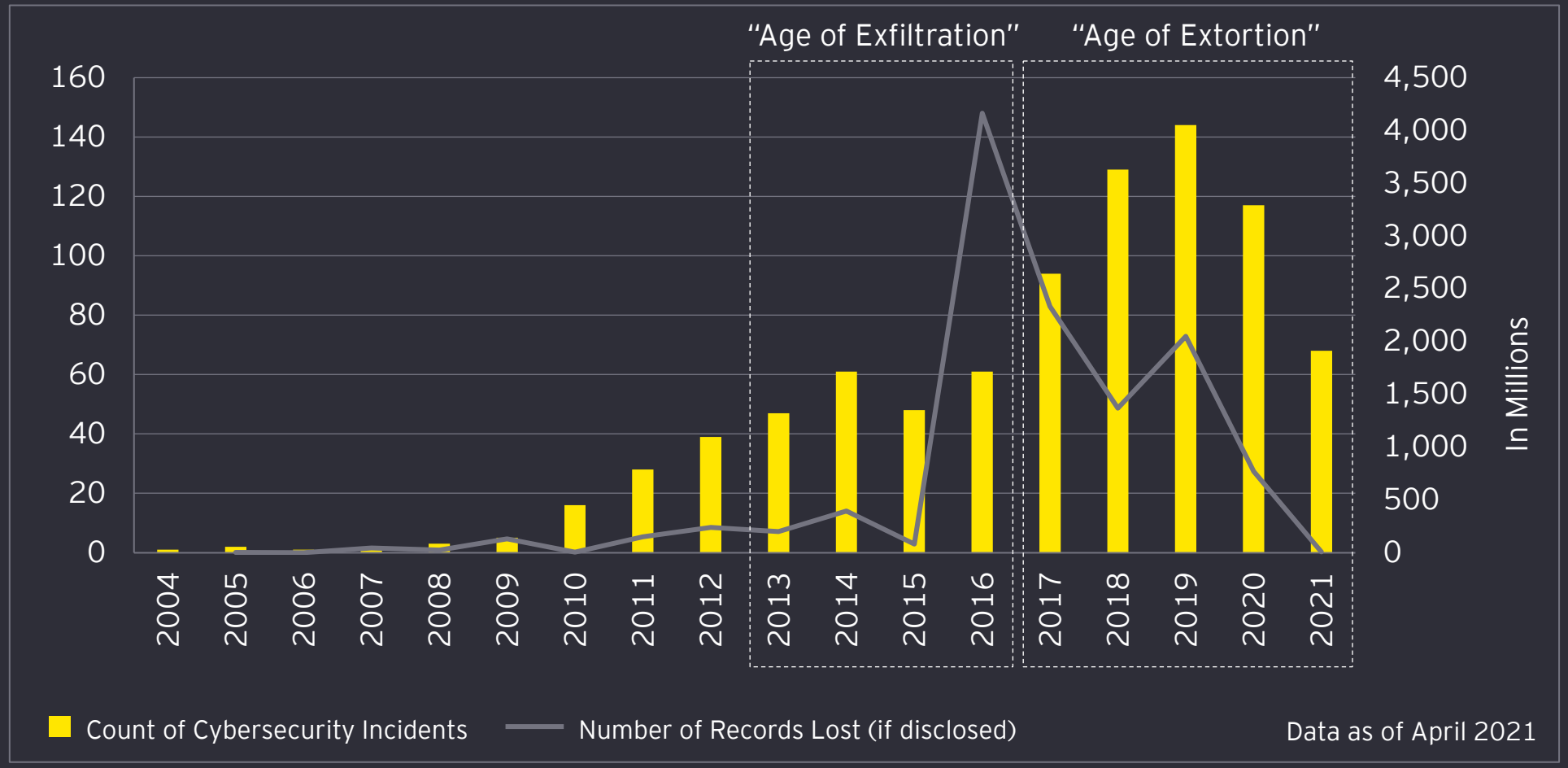
# Cyber threats continue to evolve and increase cyber risk exposure



# Cybersecurity incidents are on the rise and billions of records are lost each year

- "Double extortion" ransomware has significantly increased over the past 2 years
- Cyber insurance premiums are on the rise (↑20%-50%) and some may no longer cover extortion pay-outs to criminals
- Cyberattacks have become far more destructive
- An increasing number of companies are not able to recover critical data or systems

## Publicly Reported Cybersecurity Breaches and Total Records Lost






ForgePoint CAPITAL

EY

# Shadow investigations have increased five-fold since 2020

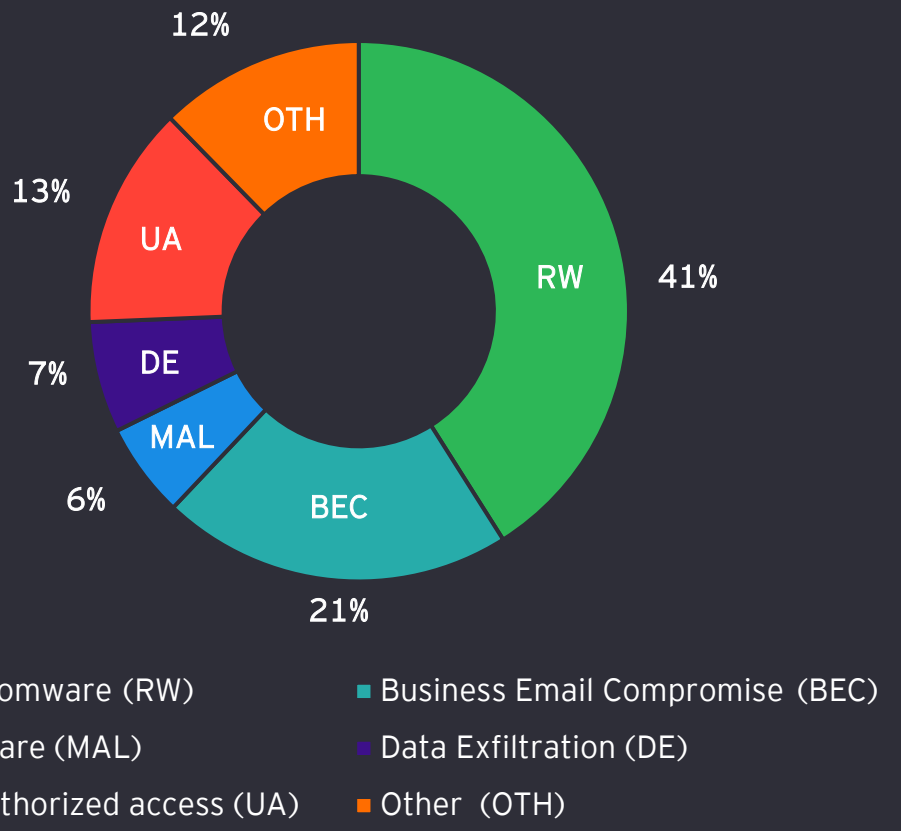
## Ransomware trends

- Ransom paid now routinely in millions
- Significant gaps in resiliency and a big disconnect with business continuity and disaster recovery plans
- Large majority of the attacks focused on Windows AD
- Insurance coverage is a large factor in payment
- Theft of [old] unstructured data is increasing
- Strong monitoring and expedited response are key to mitigating the impact

## Business email compromise trends

- Multi-factor authentication and zero trust architecture not deployed in email environments
- Switch routing of payables, receivables, or payroll
- Suspicious geographic monitoring and email box rule detection helps with response

## Shadow Investigations* By Incident Type

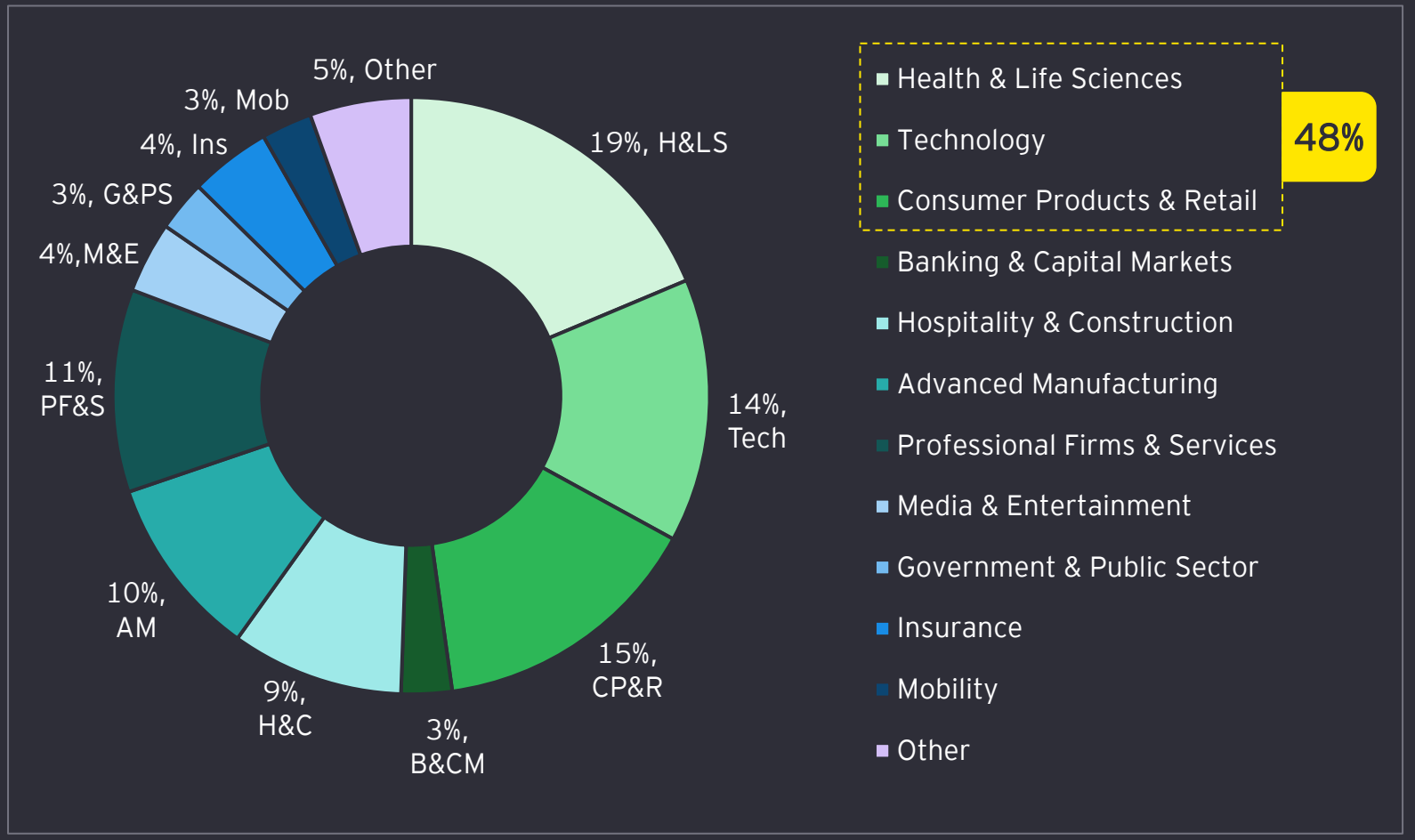



*Independent forensic investigation of a cyber incident or breach by a company's external audit firm*

# Threat actors are opportunistic and generally target companies likely to pay

- Three sectors comprise nearly 50% of the recent shadow investigations:
  - Health and Life Sciences
  - Technology
  - Consumer Products and Retail
- But no sector is immune!
- Don't discount the perceived value of the data in your organization
- You may not be the target, but rather a means of getting to the real target
- Increase in supply chain attacks
- Preparation is key; those who trained and exercised their program were able to limit the damage

## Shadow Investigations by Industry



# 2

# 5 common themes in security program assessments

# Polling question 3

At a high level, how would you rate your organization's (or clients' organizations) overall cybersecurity maturity?

A Level 0: Incomplete – Ad hoc, unknown, and mostly incomplete

B Level 1: Initial – Unpredictable and reactive

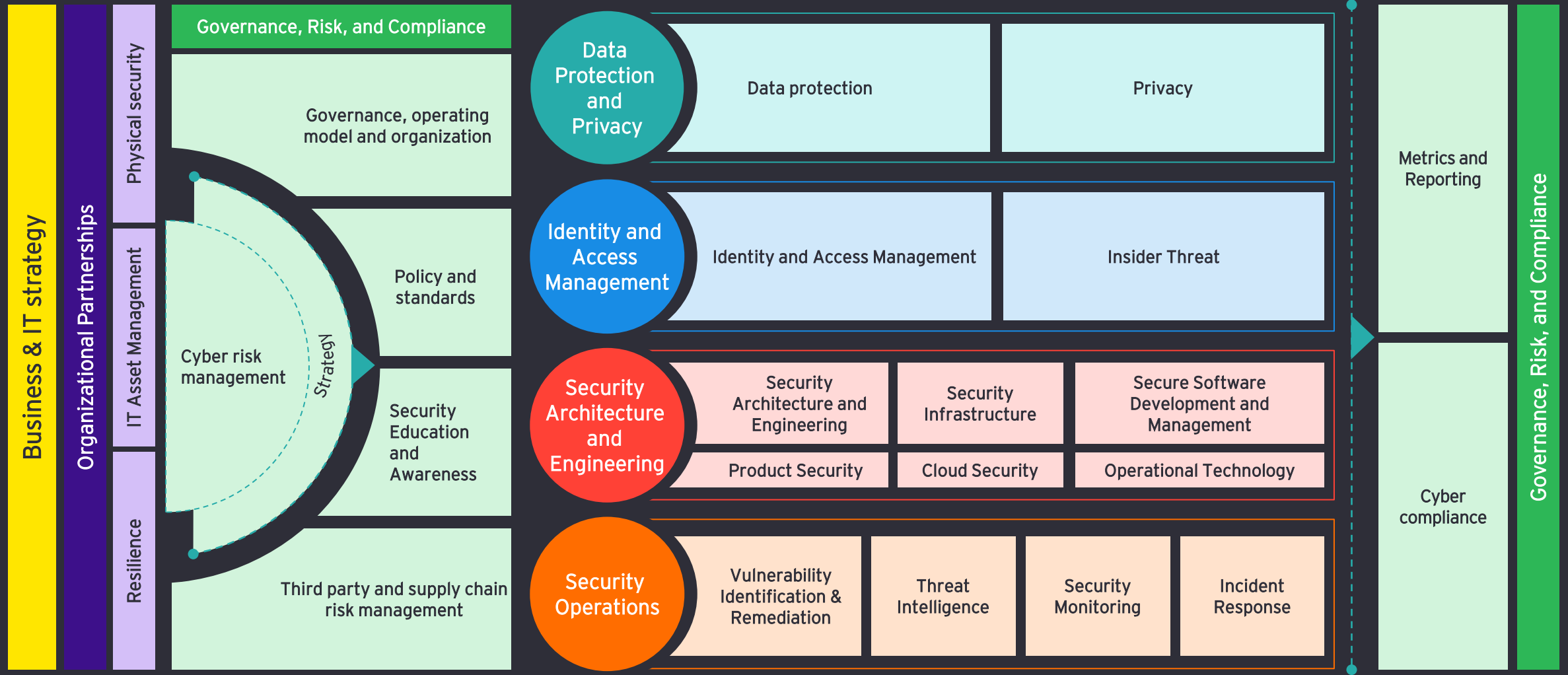
C Level 2: Managed – Managed at the individual capability level

D Level 3: Defined – Proactive and anticipates needs and changes

E Level 4: Quantitatively Managed – Measured, controlled, and verified

F Level 5: Optimizing – Stable, flexible, and continuously improving

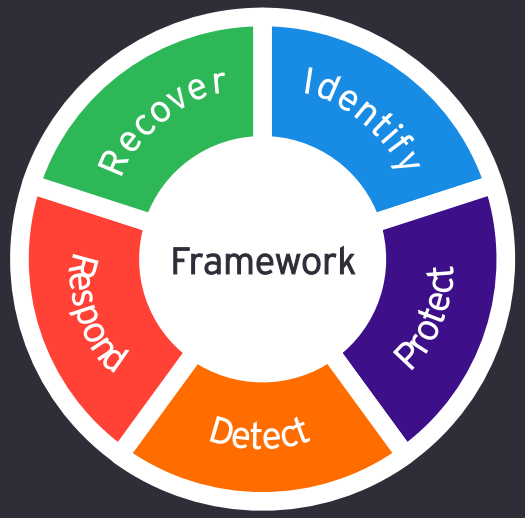
# A framework for evaluating cybersecurity programs



# Companies are relatively good at assessing, identifying risk, and building roadmaps...

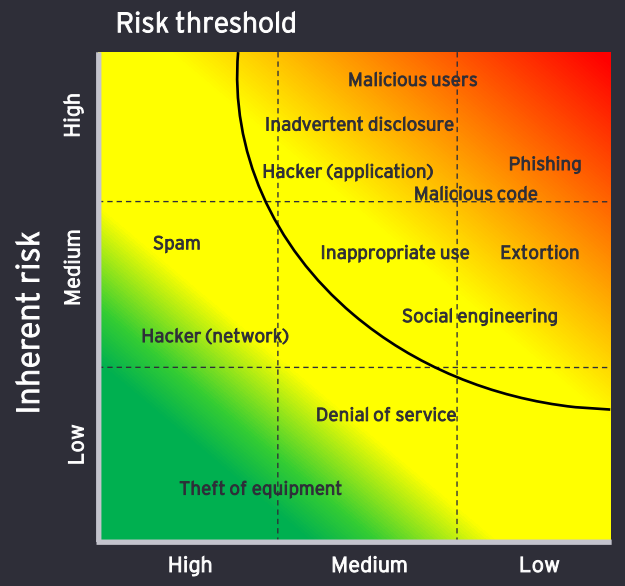
1 2 3 4 5

## Cyber framework and capabilities assessment

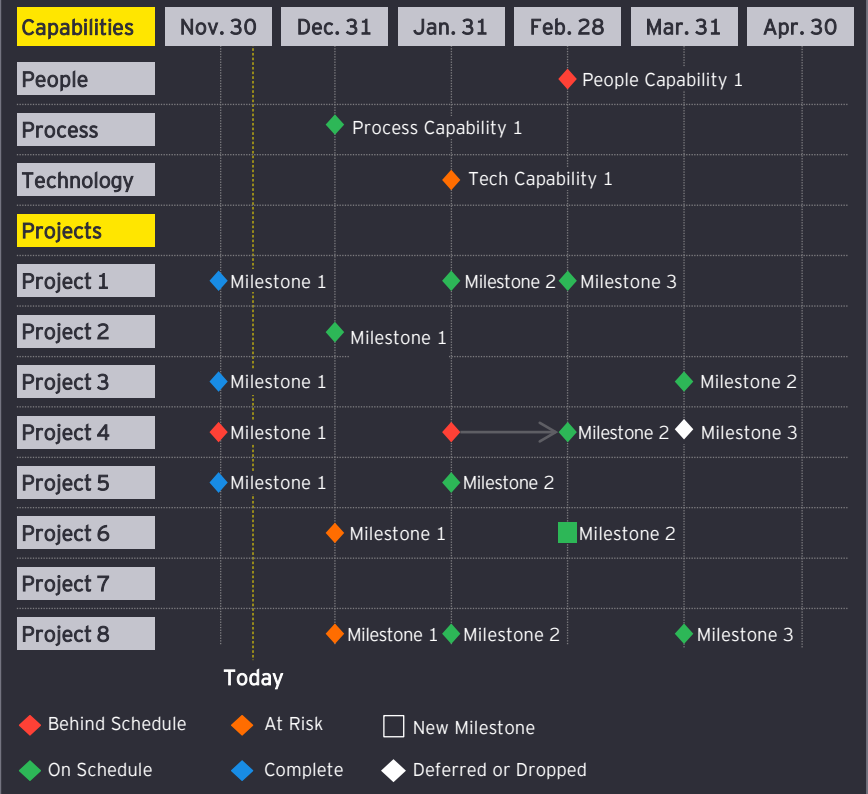



NIST Cybersecurity Framework (CSF)

## Risk and controls effectiveness analysis




## Strategy and initiative or investment roadmap




**Notes:** 1 Footnote text, 2 Footnote text, 3 Footnote text, 4 Footnote text, 5 Footnote text



ForgePoint CAPITAL

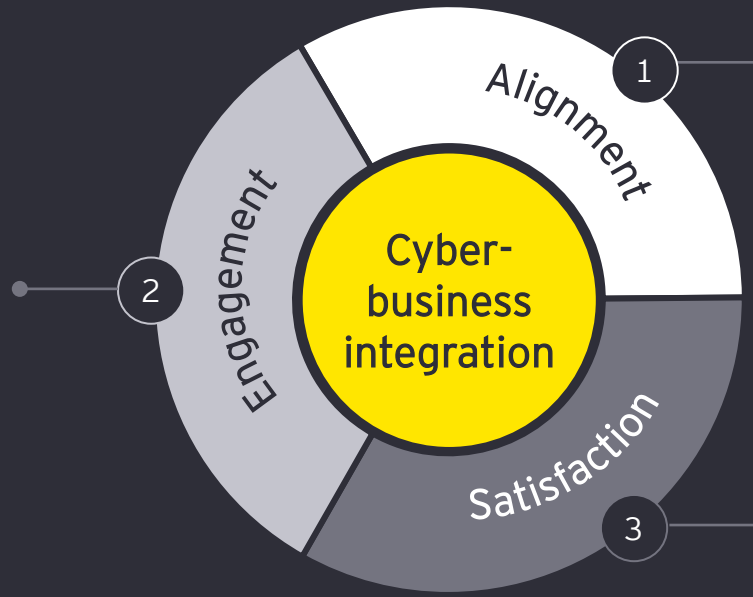
EY

# But they often overlook three critical elements for effective cyber-business integration

1
2
3
4
5

**Engagement** and communication mechanisms with business stakeholders

- Service catalog with engagement mechanism and cost chargeback
- Communication and governance channels (bi-directional)
- Performance reporting mechanisms




**Alignment** to business goals and objectives

- Mapping of cyber strategy to business and IT strategy
- Establish risk profile to align to business goals and anticipate needs
- Apply appropriate levels of controls to protect the things that matter most

**Satisfaction** with performance and delivery of security services

- Feedback loops from the business and key stakeholders
- Escalation paths when adjustments and attention is needed
- Recognition for exceptional performance and service



ForgePoint CAPITAL

EY

# Security architecture must "look everywhere"

1

2

3

4

5

**Look Left** (West)

- Secure SDLC and DevSecOps
- Security and privacy by design
- Certifications and continuous testing assurance (as a testing *producer*)

**Look Right** (East)

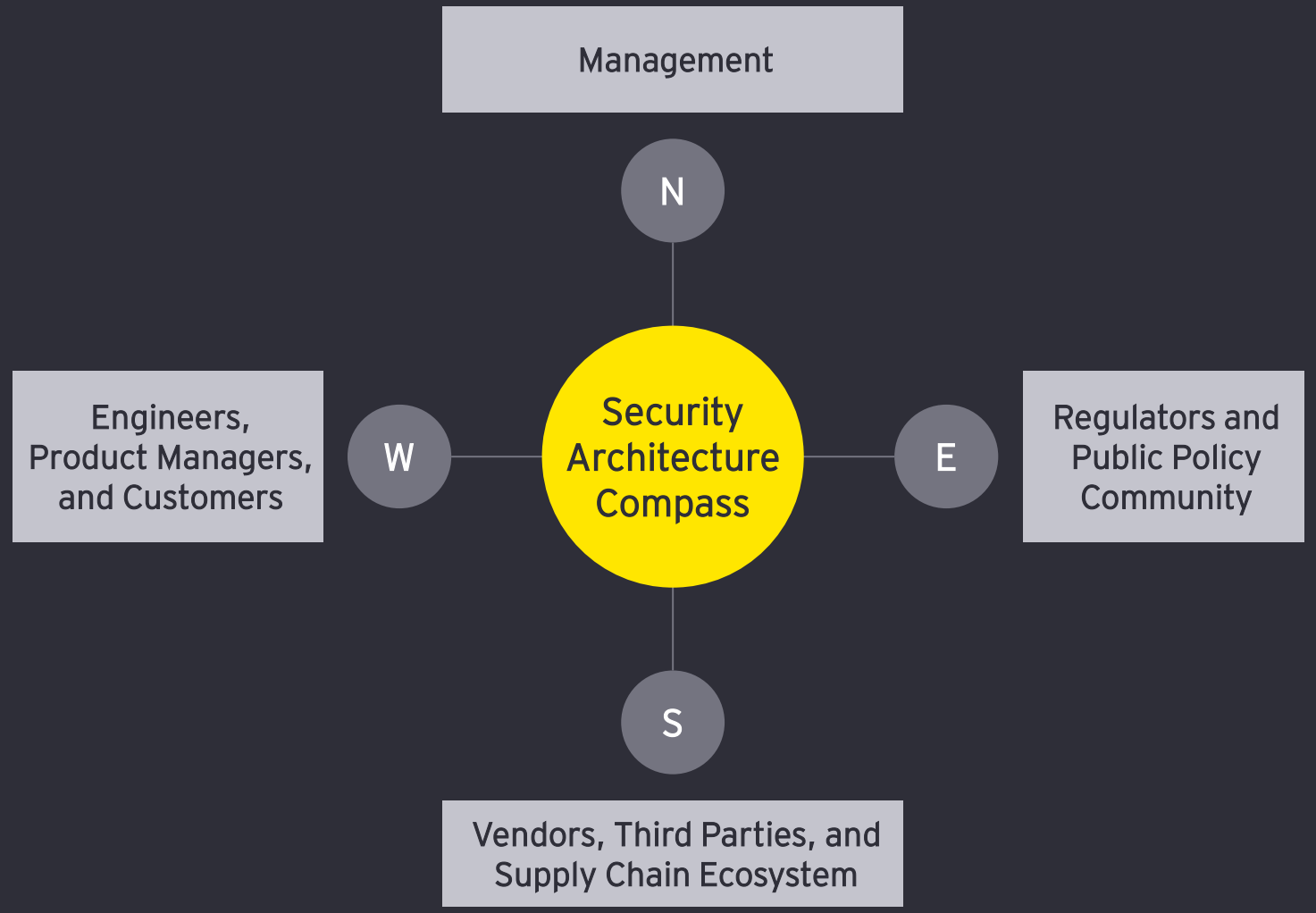
- Certifications and attestations
- Proactive regulatory "mappings" and transparent regulatory response

**Look Up** (North)

- Reporting, communications, visibility and accountability
- Budgeting and resource allocation

**Look Down** (South)

- Enhanced standards and testing (as a testing *consumer*)
- Zero trust architecture



# Traditional third-party risk management programs do not protect against supply chain attacks

1

2

3

4

5

Company identifies a business need and decides to procure software or services from a third-party

# Traditional third-party risk management programs do not protect against supply chain attacks

1

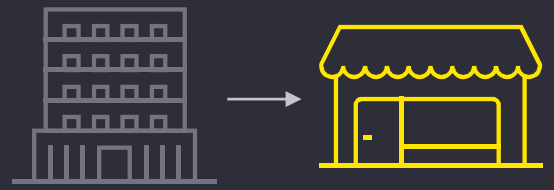
2

3

4

5

Vendors compete and eventually a service provider or solution is selected (and sometimes is a factor in the selection)



# Traditional third-party risk management programs do not protect against supply chain attacks

1

2

3

4

5

Vendor security questionnaire is submitted to the vendor by the company

# Traditional third-party risk management programs do not protect against supply chain attacks

1

2

3

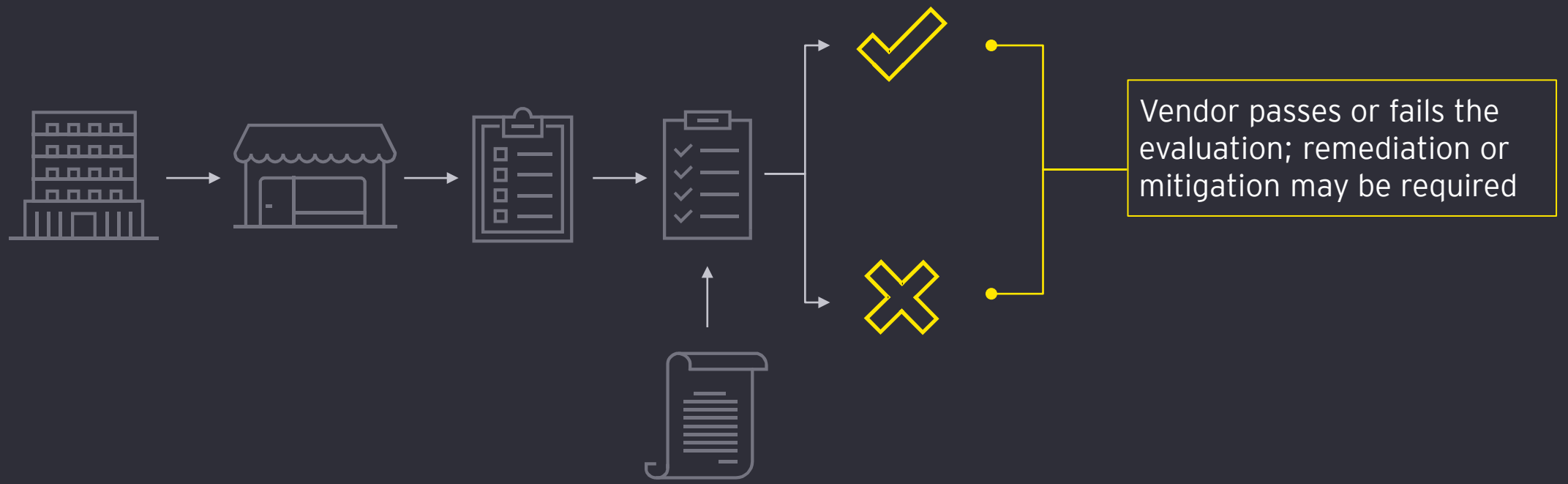
4

5

Vendor completes questionnaire and submits required evidence, certifications, or documentation

# Traditional third-party risk management programs do not protect against supply chain attacks

1
2
3
4
5



Vendor passes or fails the evaluation; remediation or mitigation may be required

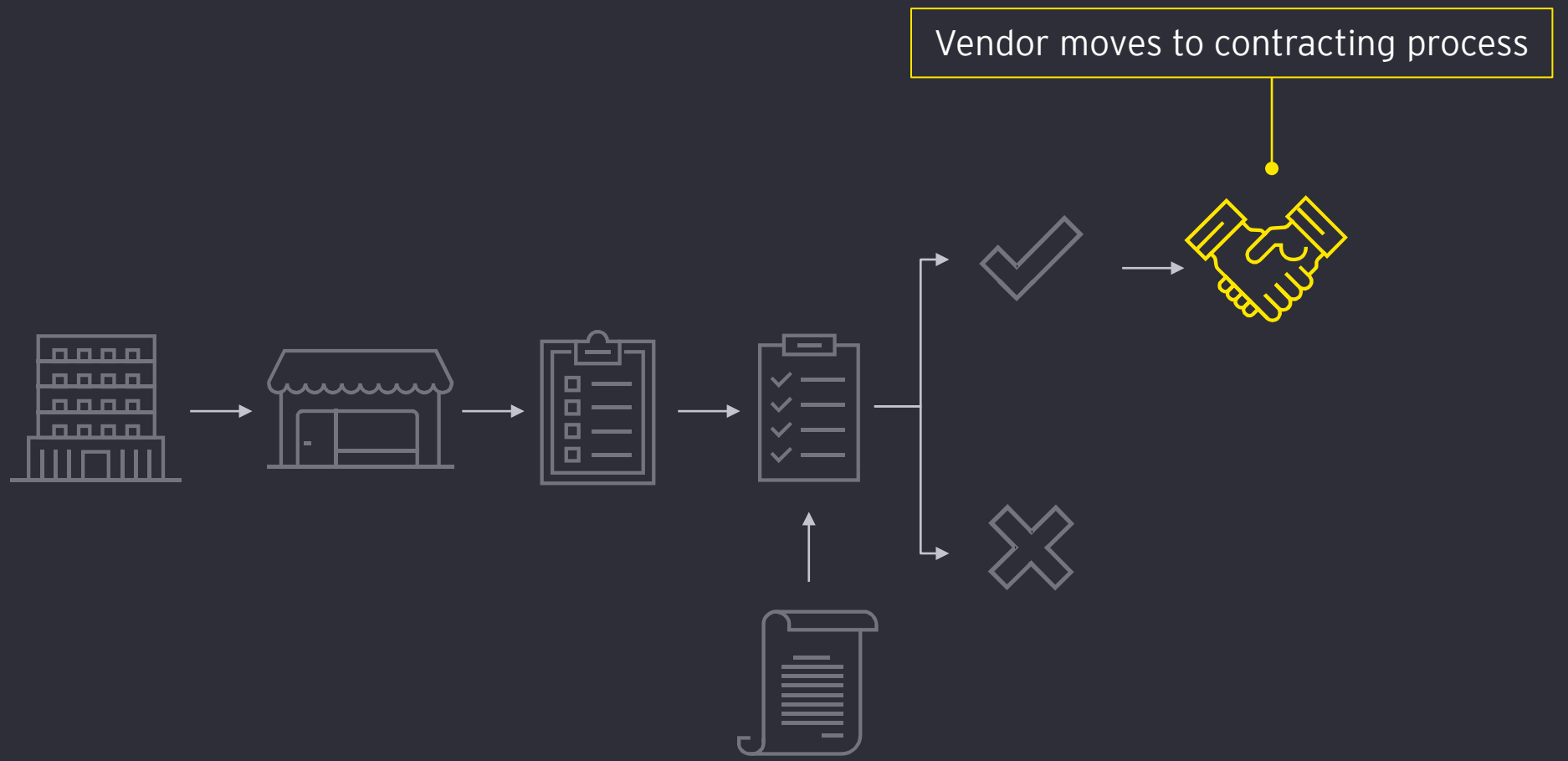


ForgePoint CAPITAL

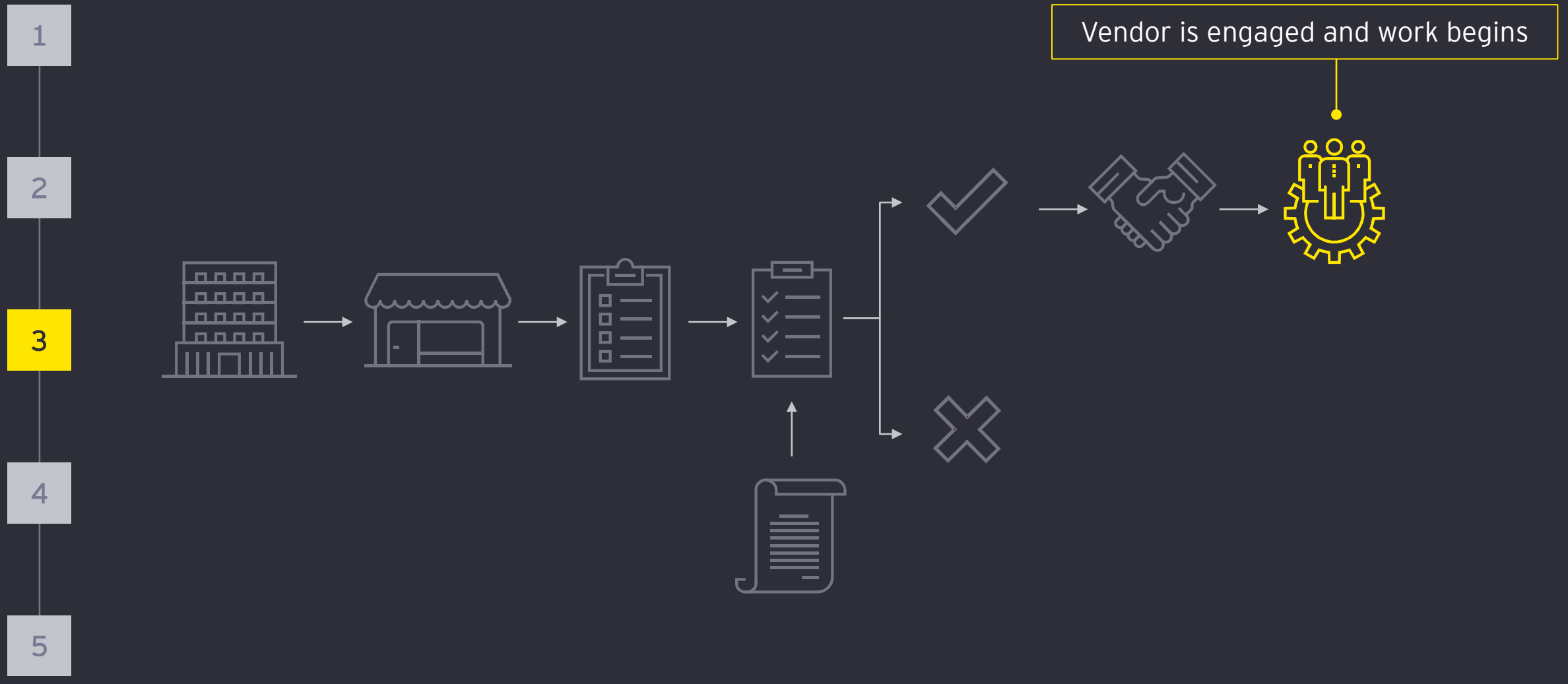
EY

# Traditional third-party risk management programs do not protect against supply chain attacks

1
2
3
4
5

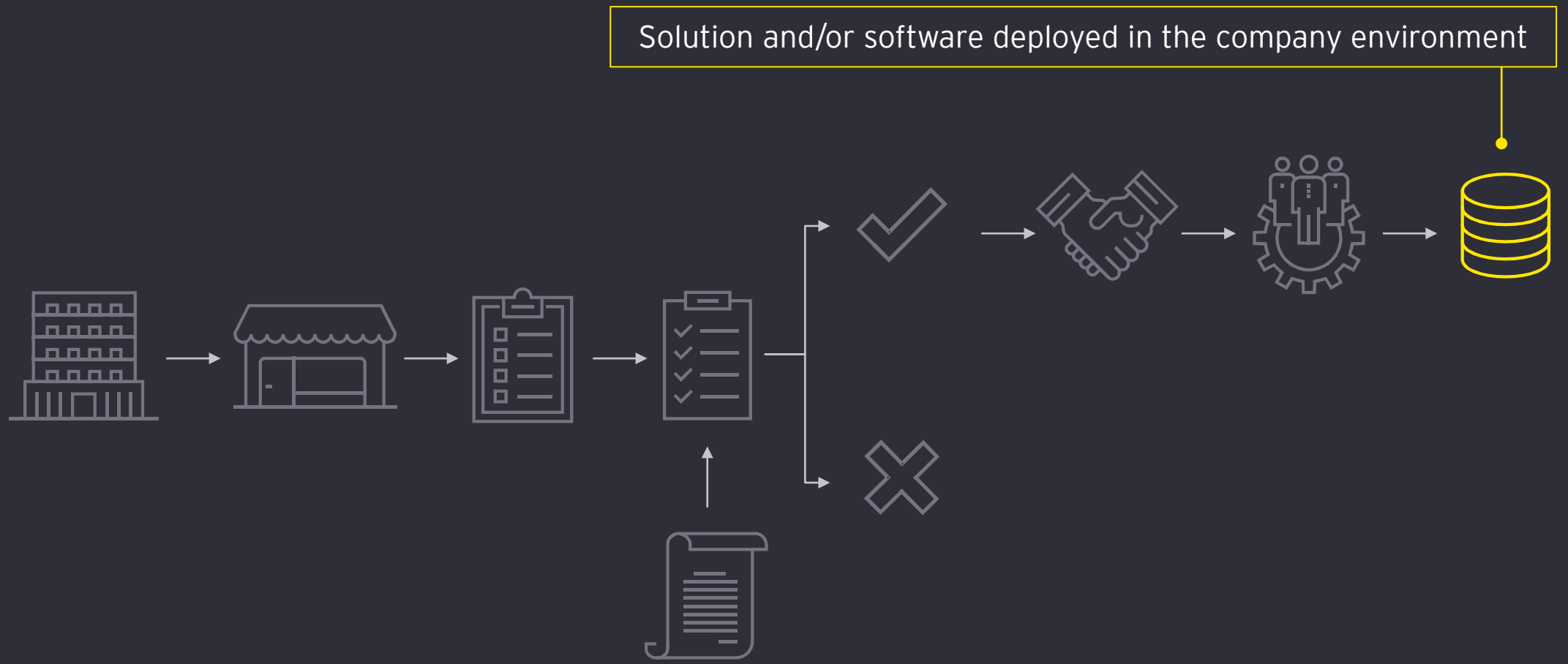


# Traditional third-party risk management programs do not protect against supply chain attacks



# Traditional third-party risk management programs do not protect against supply chain attacks

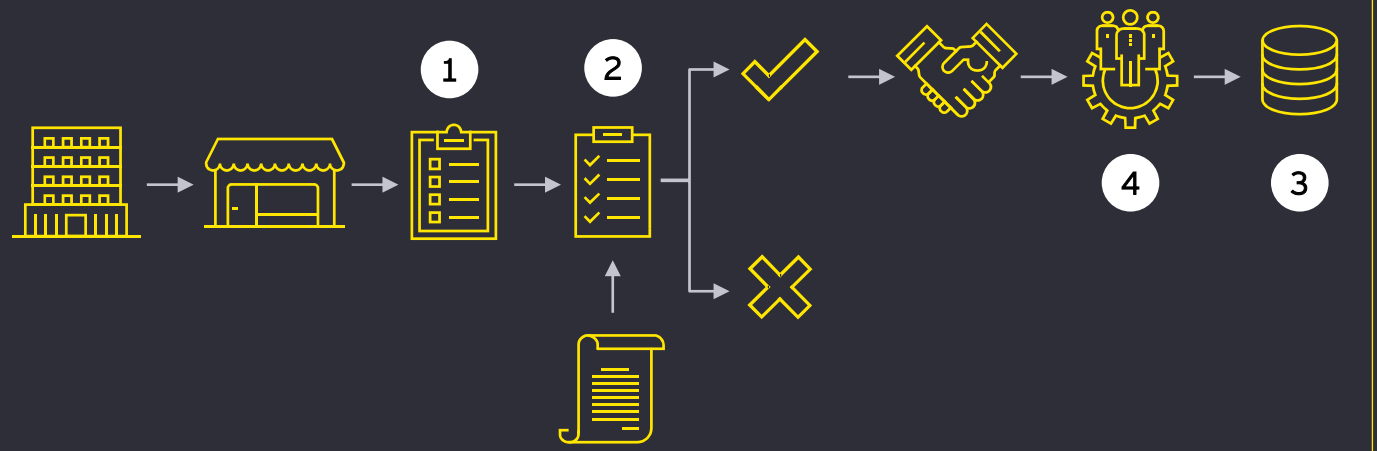
1
2
3
4
5



# Traditional third-party risk management programs do not protect against supply chain attacks

1
2
3
4
5

1. Questionnaires and certifications ≠ code/solution testing
2. Ongoing testing (periodic & triggered) > point-in-time evaluations
3. If vendors do not test their code/solutions *with each release*, you must. If they do, make them prove it; and you should likely reperform the testing in your environment anyway…
4. Nth-parties (vendors of vendors) pose just as big a risk as the primary vendor




**Third-party security risk management basic hygiene checklist**

- ☑ A complete vendor list
- ☑ Procurement channels and shadow IT
- ☑ Vendor tiering and evaluation criteria for each tier
- ☑ Evidence and documentation analysis
- ☑ Re-evaluation schedule and triggers
- ☑ Vendor risk monitoring and governance



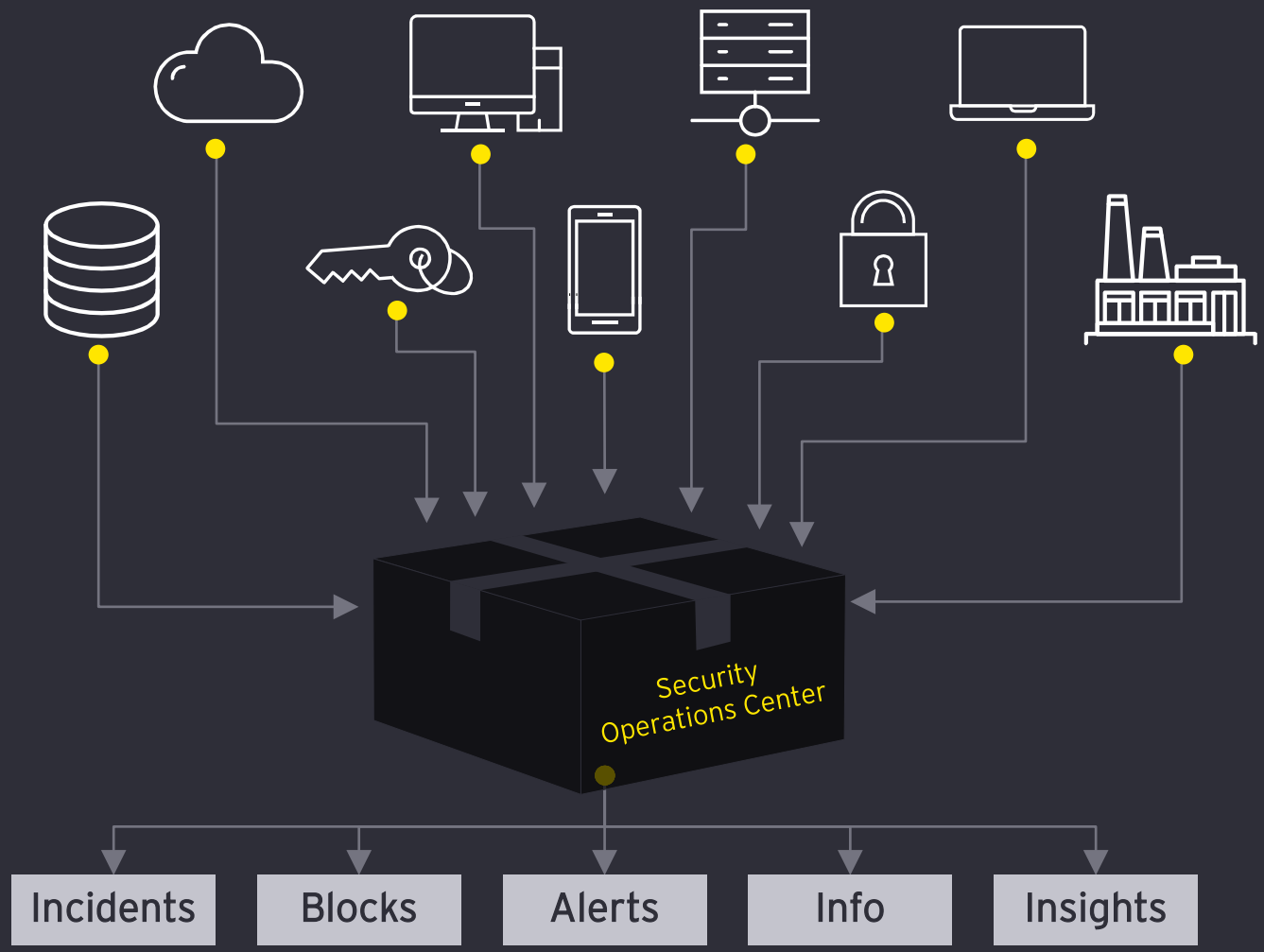
ForgePoint CAPITAL

EY

# Greater visibility and enhanced monitoring does not necessarily mean better response *(but it could)*

1
2
3
**4**
5

- Depth (type/amount of data) and breadth (BU, geographies, products, etc.) of monitoring scope
- Business stakeholder integration and system ownership
- Operational technology (OT) environments
- "Black box" SOCs (security operations centers)
- Threat hunting and active defense finds problems before they become problems
- Alert noise: qualification and investigation
- Overreliance on technology; processes playbooks and communication protocols
- Level 3 hand-offs, especially for MSSPs
- Automation versus manual processes; get ready for huge increase in volume






ForgePoint CAPITAL

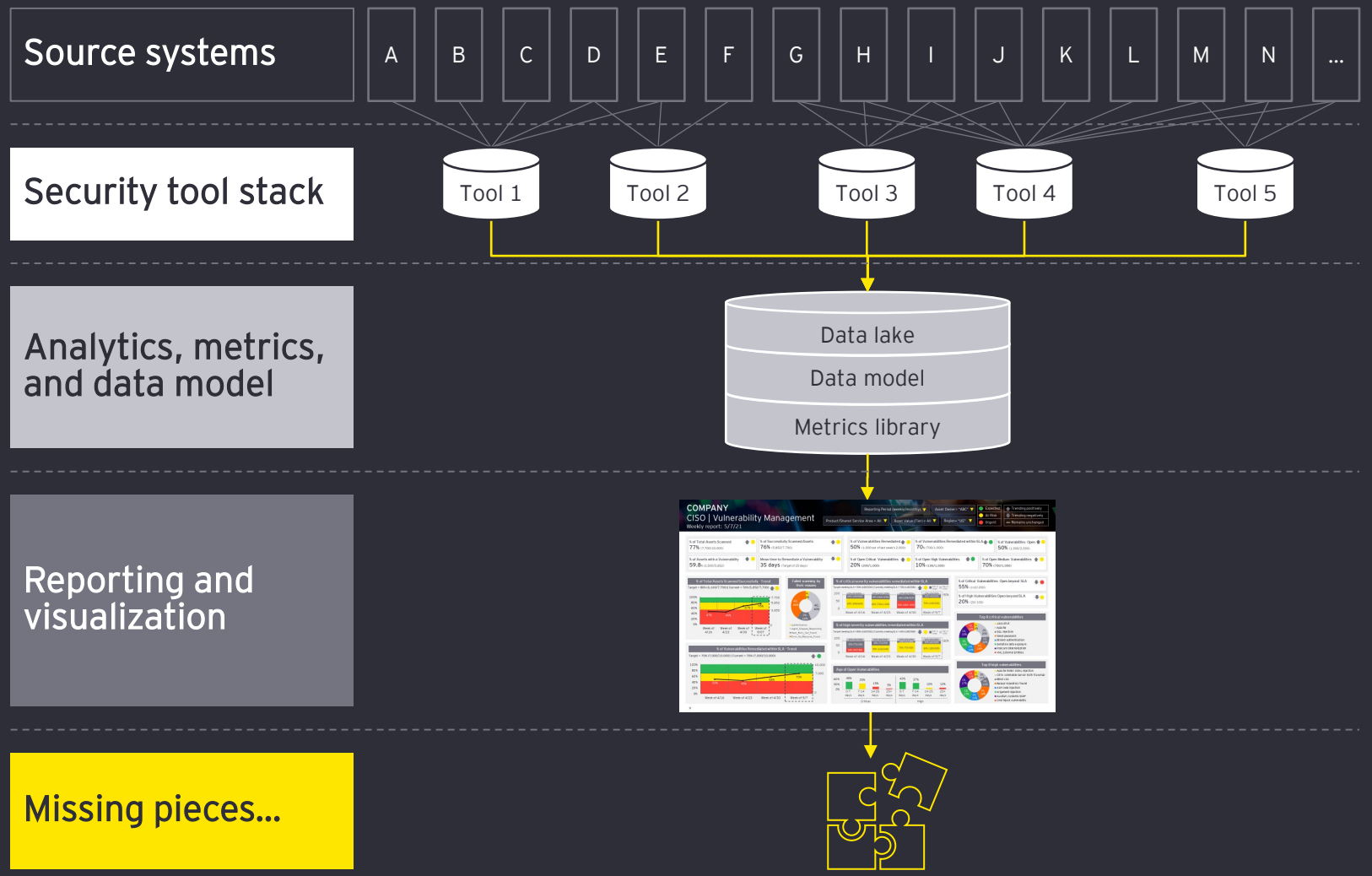
EY

# Cyber reporting, metrics, and dashboarding is missing some critical elements before it can elevate cyber maturity

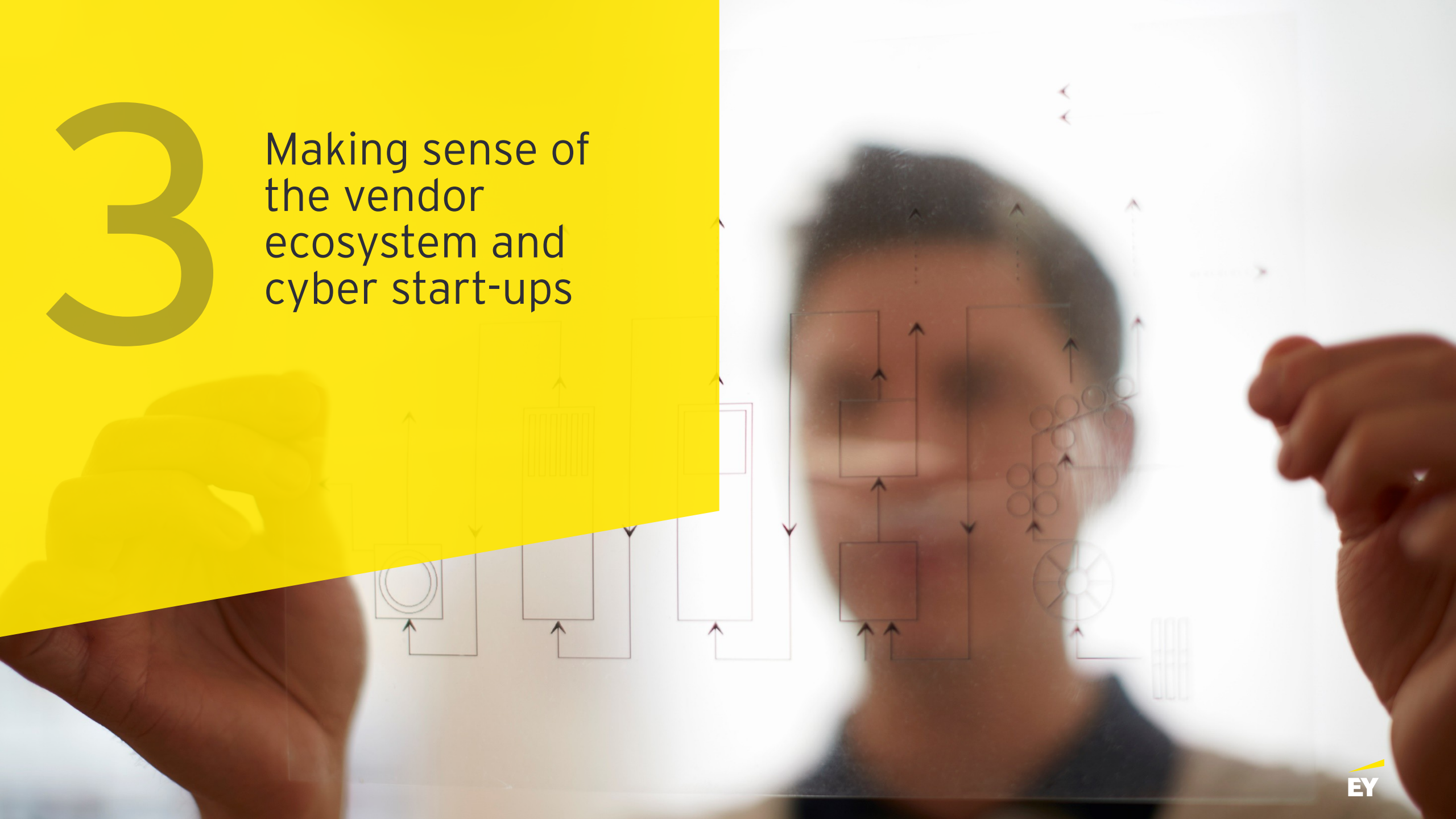
1
2
3
4
5

## Common missing pieces...

- Infusion of business context information
- Persona and audience definition
- Reporting visibility and risk governance
- Interpretation in "plain language"
- Automation and notifications
- Accountability for KPIs and KRIs within defined personas
- Historical trending and future predictive modeling



# 3 Making sense of the vendor ecosystem and cyber start-ups



# Polling question 4

## In which NIST CSF domain is your organization focusing most heavily over the next year?

**A** **Identify**
Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy

**B** **Protect**
Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology

**C** **Detect**
Anomalies and Events; Security; Continuous Monitoring; and Detection Processes

**D** **Respond**
Response Planning; Incident Response Communications; Response Analysis; Mitigation; and Improvements

**E** **Recover**
Recovery Planning; Restoration Improvements; and Recovery-Based Communications

# Next Evolution of NIST's Framework

| Landscape Overview | | | | |
|---|---|---|---|---|
| | Identify | Protect | Detect | Respond/Recover |
| Endpoint | | | | |
| Network | | | | |
| Application | | | | |
| Data | | | | |
| Identity | | | | |

- Simplify NIST's five categories into four
- Adding a second dimension helps to make CSF "real"
  - Credit to the Cyber Defense Matrix for the original inspiration
- Framework can also be used to show a maturing security program (Green, Yellow, Red)



ForgePoint CAPITAL

EY

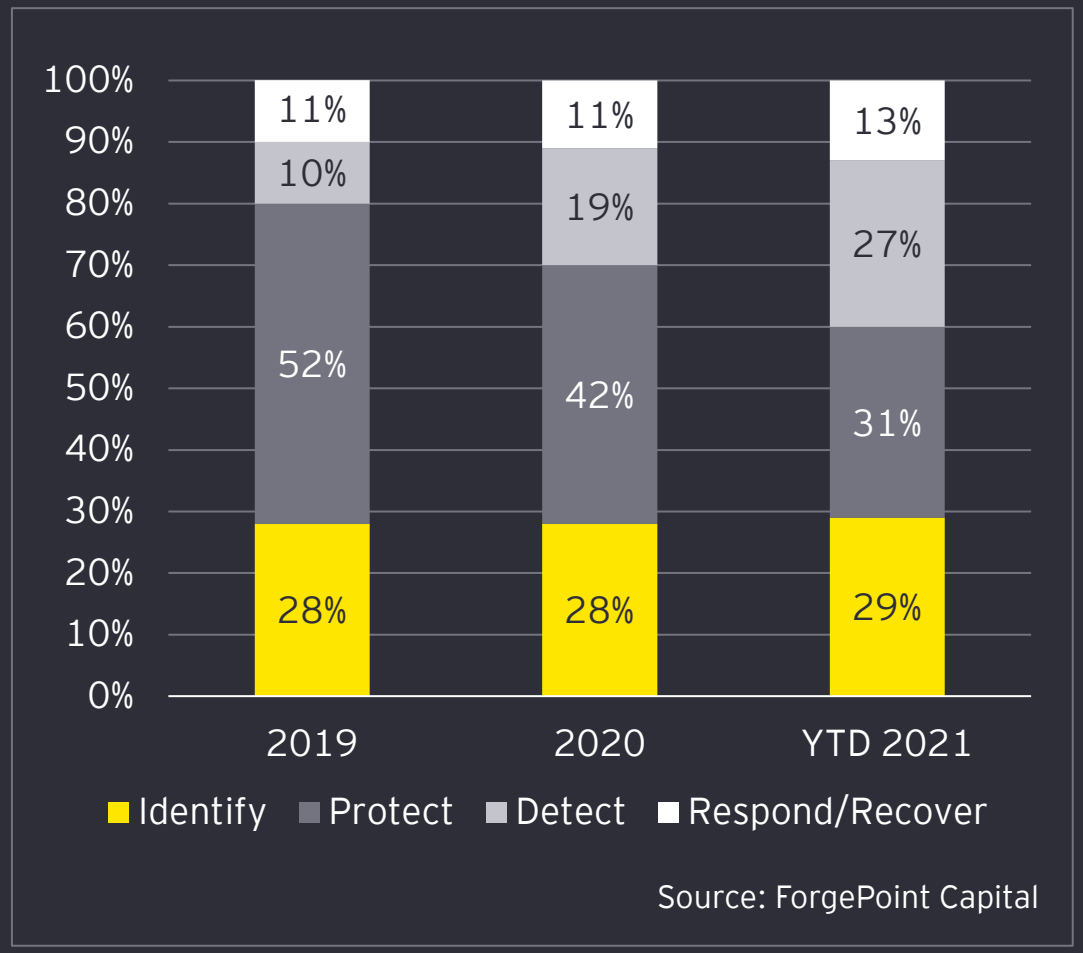
# Applying the framework in the leadership setting

| Security Program at Current State | | | | |
|---|---|---|---|---|
| | Identify | Protect | Detect | Respond/Recover |
| Endpoint |  |  |  |  |
| Network |  |  |  |  |
| Application |  |  |  |  |
| Data |  |  |  |  |
| Identity |  |  |  |  |

- "Based on the risks unique to our company and industry, I believe the red items are our current gaps and lowest hanging fruit to reduce risk to our organization"
- "I'm working to change those from red to yellow, in the next 6 months and will share the new dashboard then"

# Investment by Category

Investment in innovation over time saw the largest shift from protecting to detecting




Source: ForgePoint Capital

| Landscape Overview | | | | |
|---|---|---|---|---|
| | Identify | Protect | Detect | Respond/ Recover |
| Endpoint | | | | |
| Network | | | | |
| Application | | | | |
| Data | | | | |
| Identity | | | | |

# Cyber Defense Matrix

| | Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|---|
| Devices | | | | | |
| Applications | | | | | |
| Networks | | | | | |
| Data | | | | | |
| Users | | | | | |


- Created by Sounil Yu, former Security Innovation Lead at Bank of America
- Process is critical to all types of controls
- As we move further right, increased dependency on people (i.e. SOC)

# 4 Questions and answers

# THANK YOU

Justin Greis

Will Lin

## EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.



ey.com