Cybersecurity Briefing

CFO Council

June 2021

Building a better working world

About today's speakers

Justin Greis

- Partner, Ernst & Young LLP
- Chicago, Illinois
- Global and Americas Cybersecurity Strategy, Risk, Compliance, and Resilience Leader

justin.greis@ey.com

linkedin.com/in/justingreis

justingreis.com

@JustinGreis

Michael Hinckley

- Senior Manager, Ernst & Young LLP
- Nashville, Tennessee
- Technology Risk, Compliance, and Assurance

michael.hinckley@ey.com

linkedin.com/in/michael-hinckley-ba14239

michaelhinckley.com

@hinckleysong

South Carolina Market Leaders

Jessica Donan

- Partner, Ernst & Young LLP
- Greenville, South Carolina
- Greenville Office Managing Partner, Financial Accounting Advisory Partner and US-Central Region Mobility Sector Assurance Leader

jessica.donan@ey.com

linkedin.com/in/jessica-donan

Jennifer Walker

- Senior Manager, Ernst & Young LLP
- Charleston, South Carolina
- Assurance and Consulting Services

jennifer.walker@ey.com

https://www.linkedin.com/in/jennifer-walker-6929971a6/

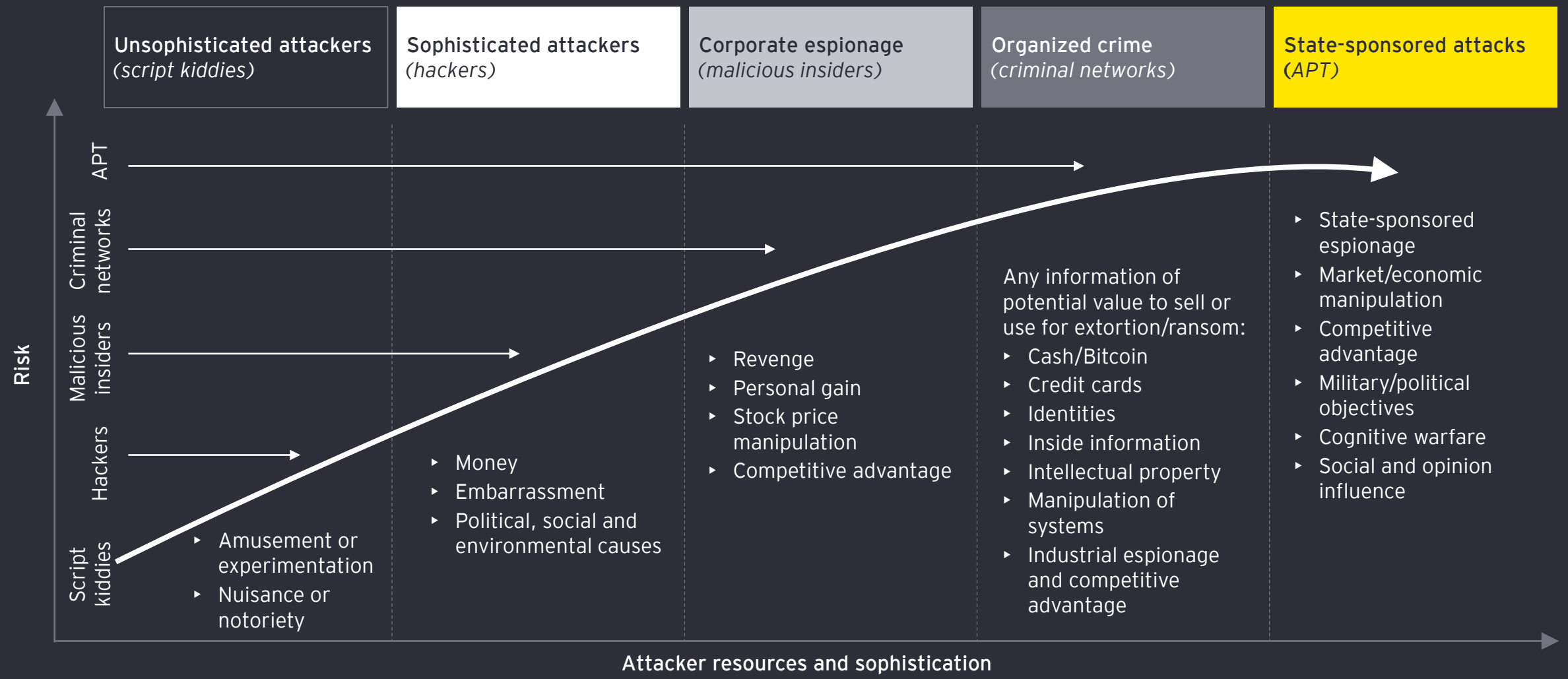
Agenda

1. Today's security landscape
2. Five common themes in cyber program assessments
3. Cybersecurity Maturity Model Certification (CMMC) update
4. Questions and answers

1

Today's security landscape

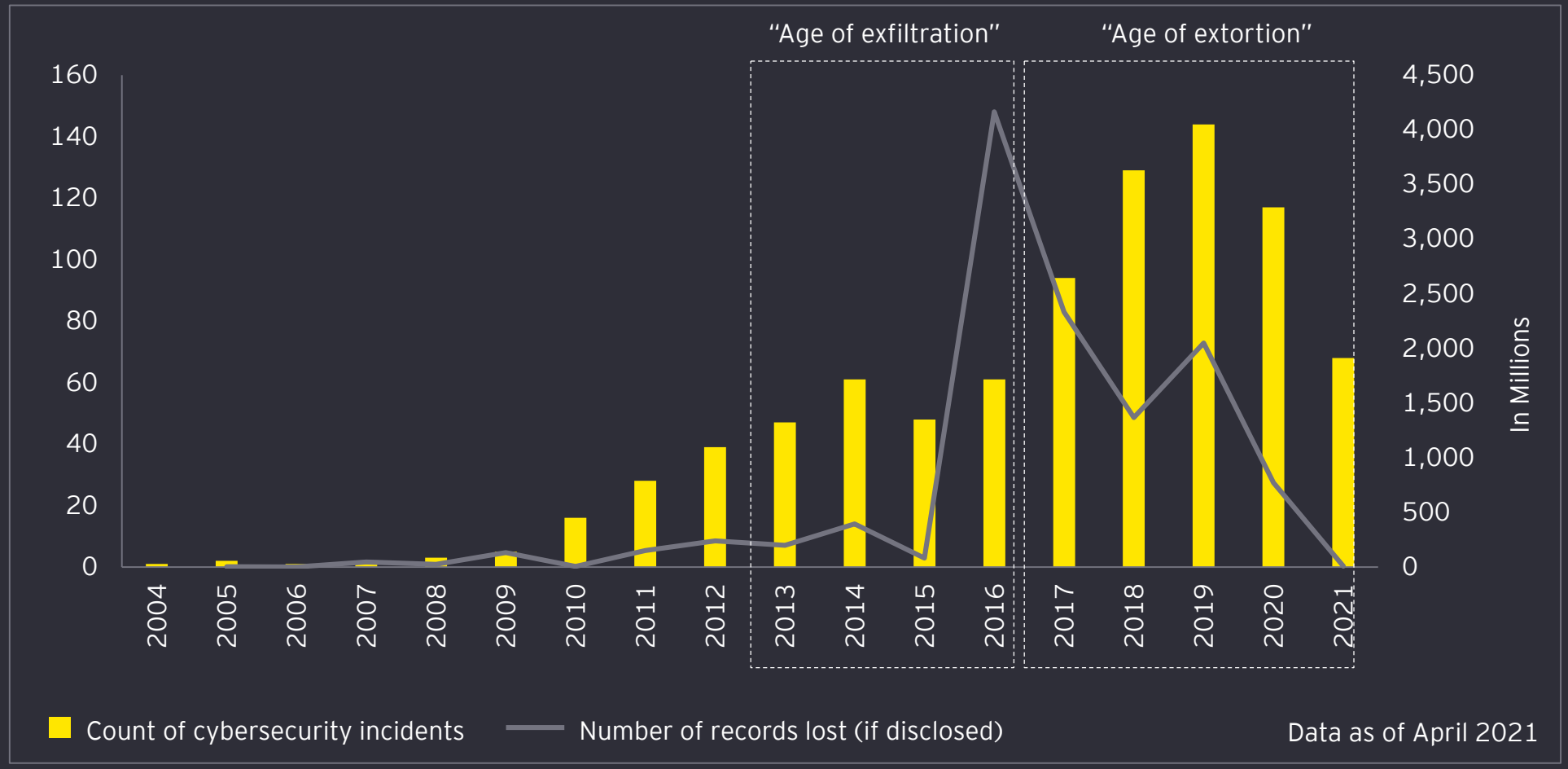
Cyber threats continue to evolve and increase cyber risk exposure



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

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

Publicly reported cybersecurity breaches and total records lost



Shadow investigations have increased five-fold since 2020

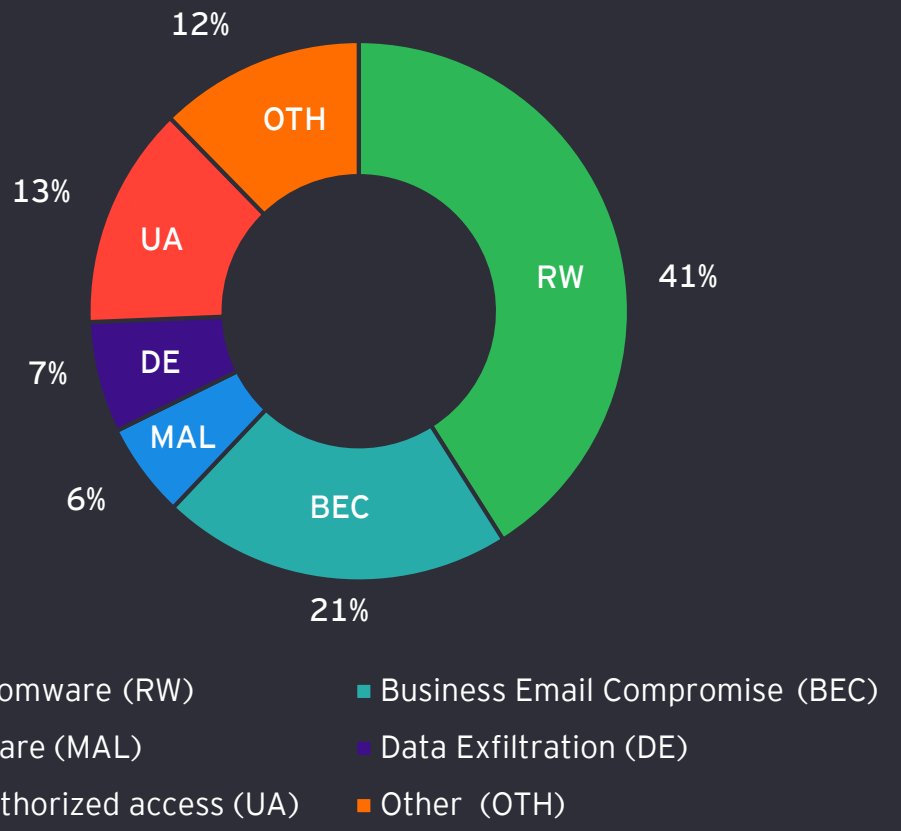
Ransomware trends

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

Business email compromise trends

- Multifactor 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

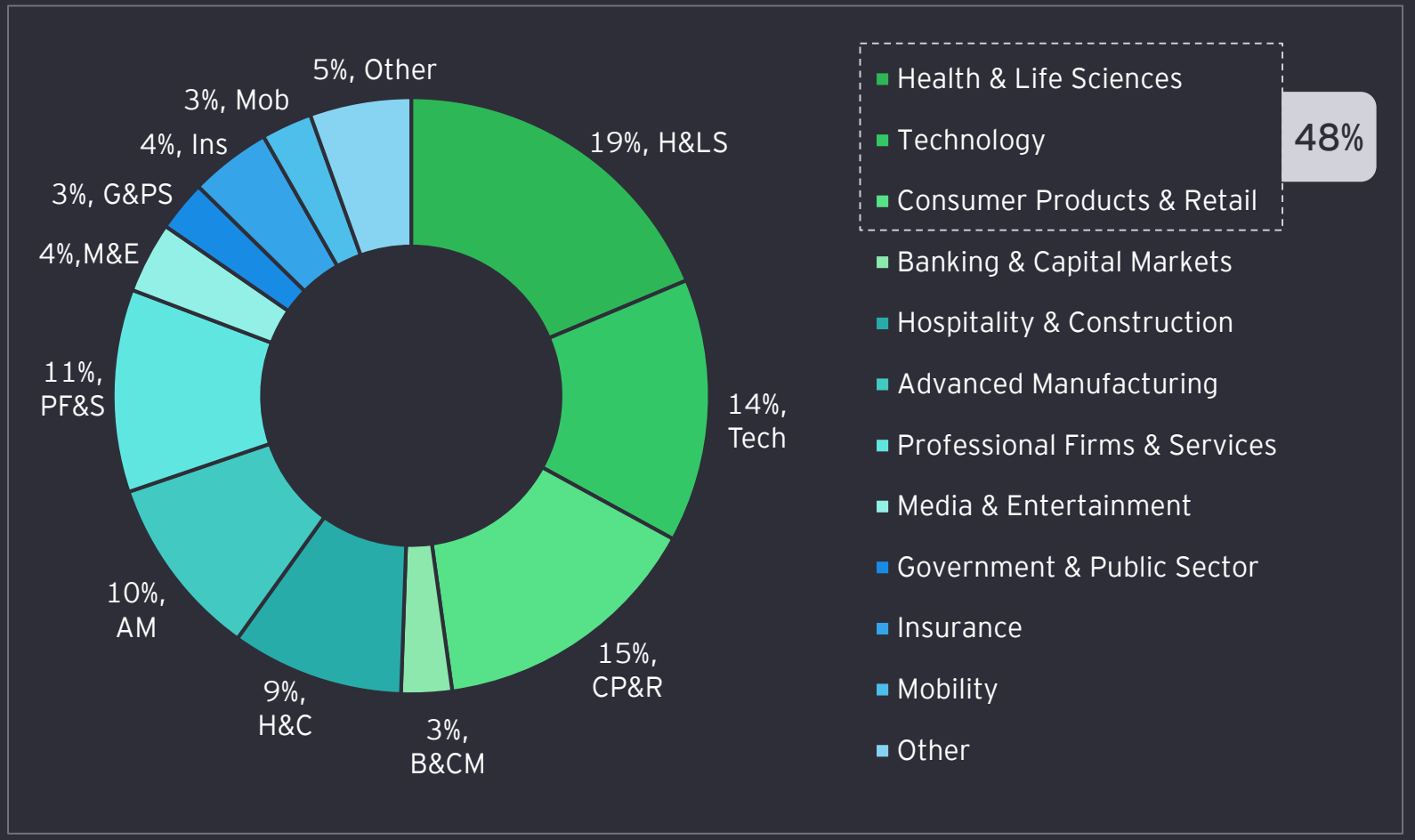


Independent forensic investigation of a cyber incident or breach

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
- 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.
- There is an increase in supply chain attacks.
- Preparation is key: those who trained and exercised their program were able to limit the damage.

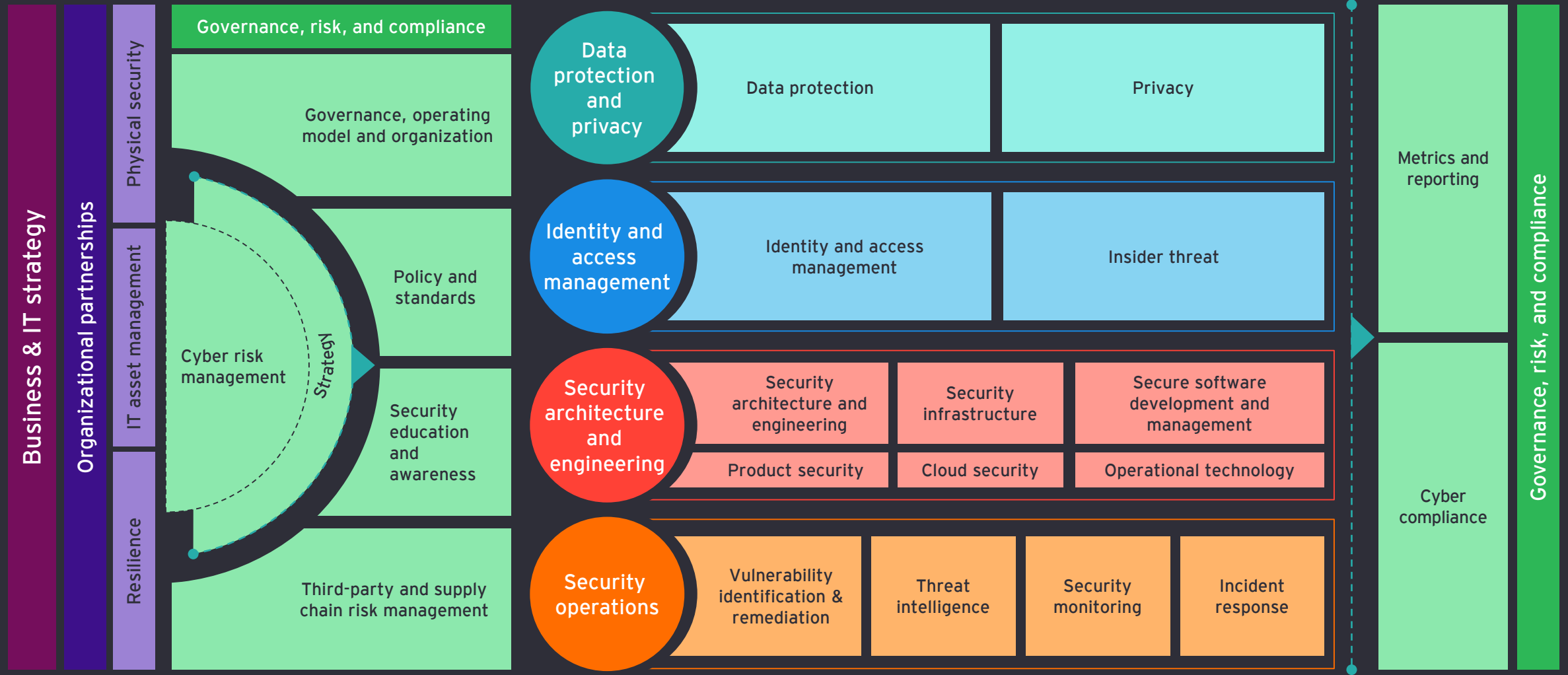
Shadow investigations by industry



2

Five common themes in cyber program assessments

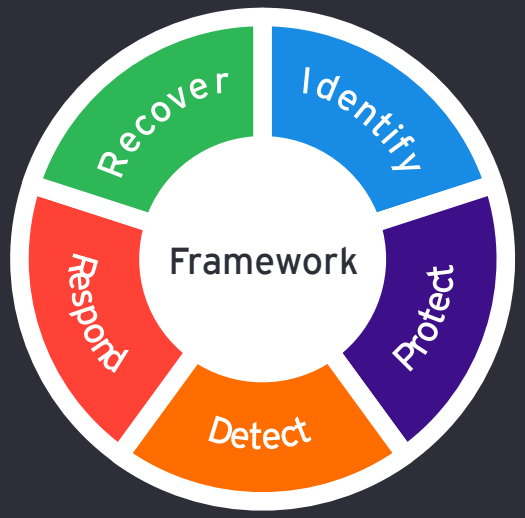
A framework for evaluating cybersecurity programs



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

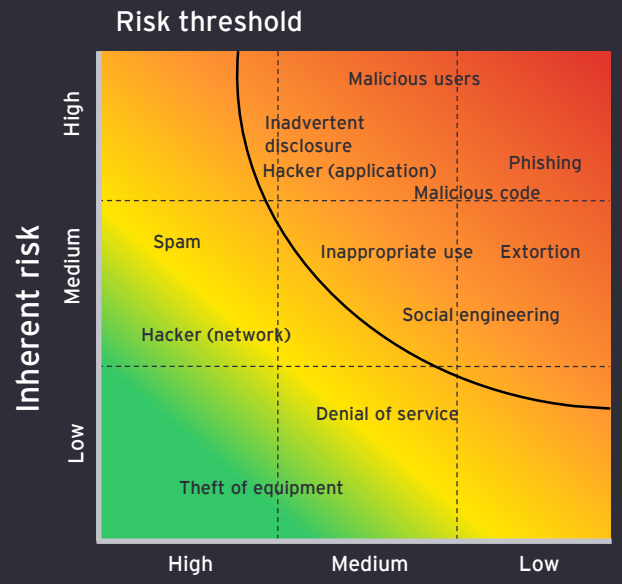
1 2 3 4 5

Cyber framework and capabilities assessment

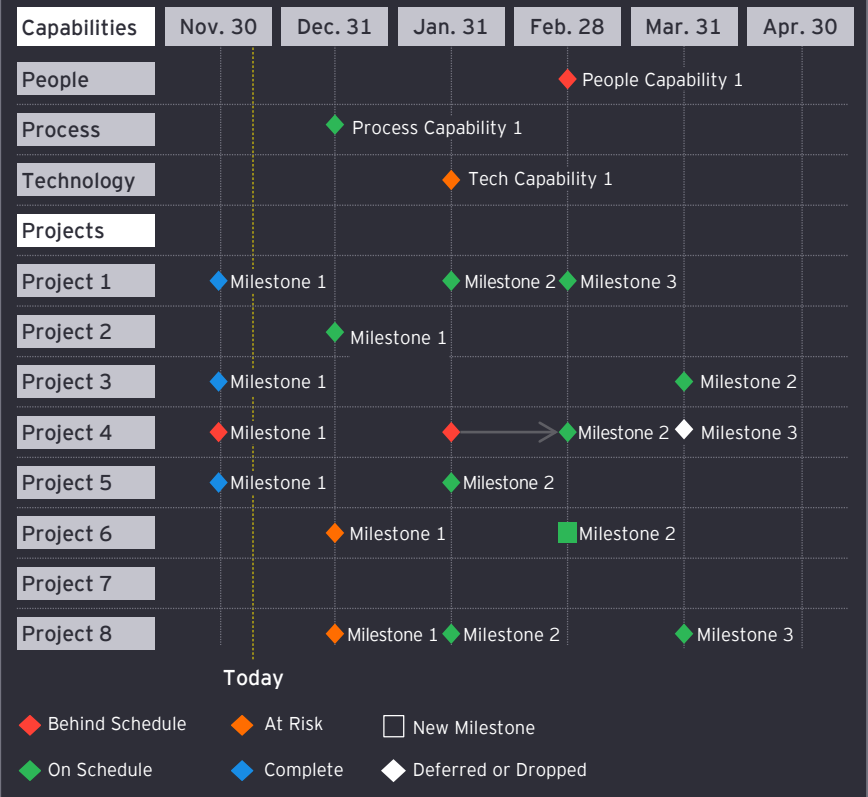


NIST Cybersecurity Framework (CSF)

Risk and controls effectiveness analysis



Strategy and initiative or investment road map



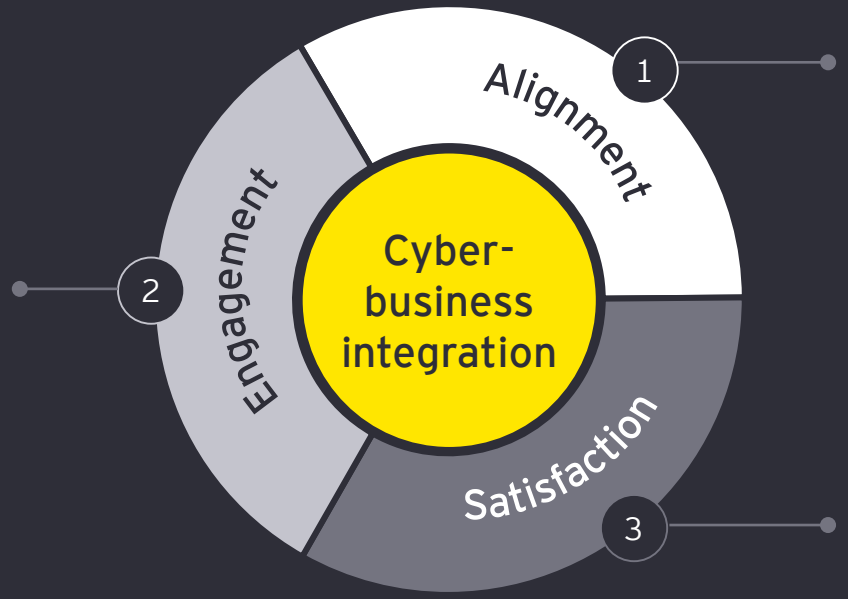
Notes: 1 Footnote text, 2 Footnote text, 3 Footnote text, 4 Footnote text, 5 Footnote text

… 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

Security architecture must "shift everywhere"

1

2

3

4

5

Shift left (West)

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

Shift right (East)

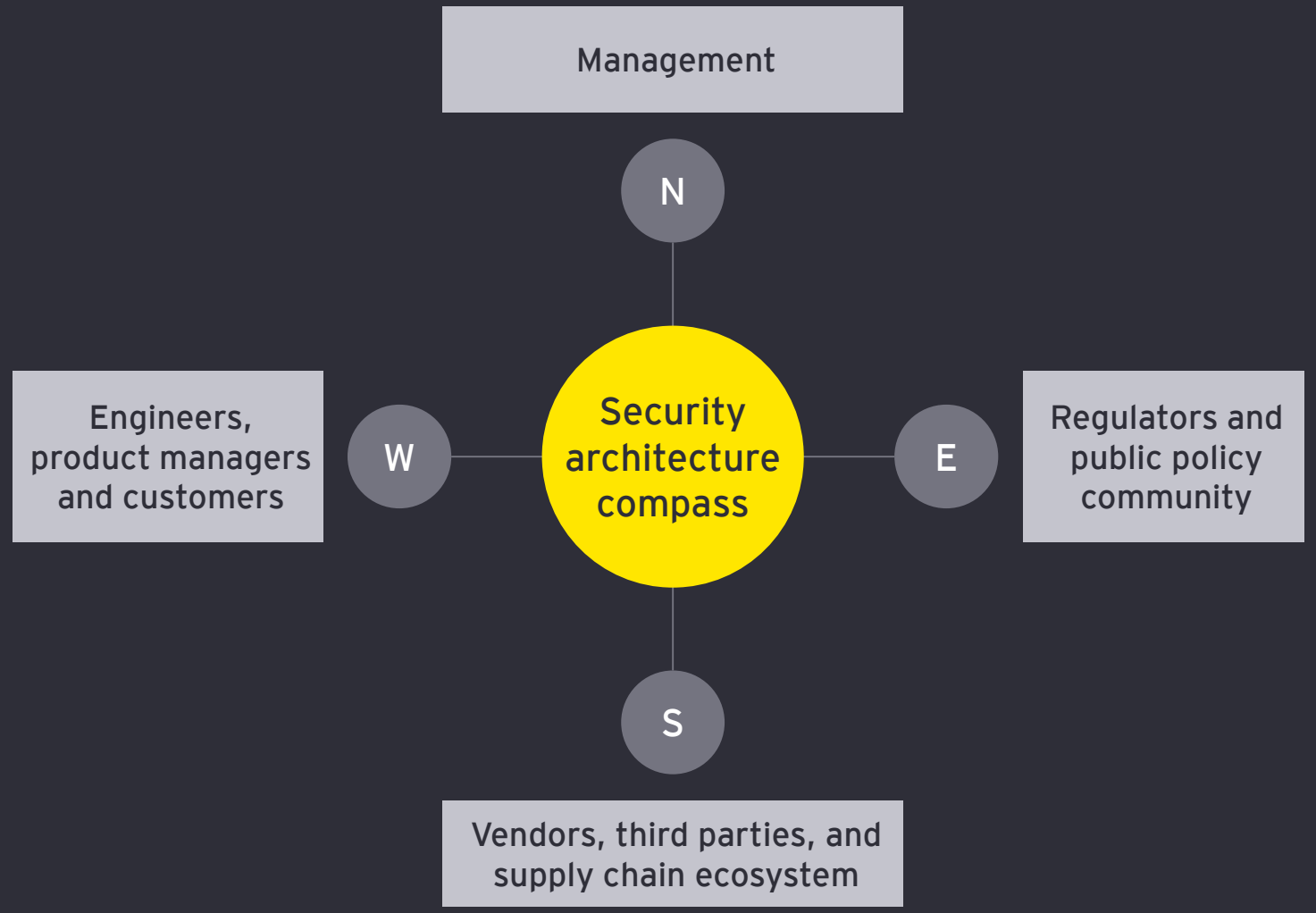
- Certifications and attestations
- Proactive regulatory "mappings" and transparent regulatory response

Shift up (North)

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

Shift 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

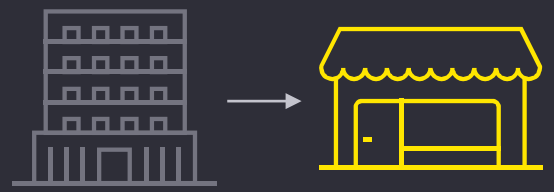
2

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

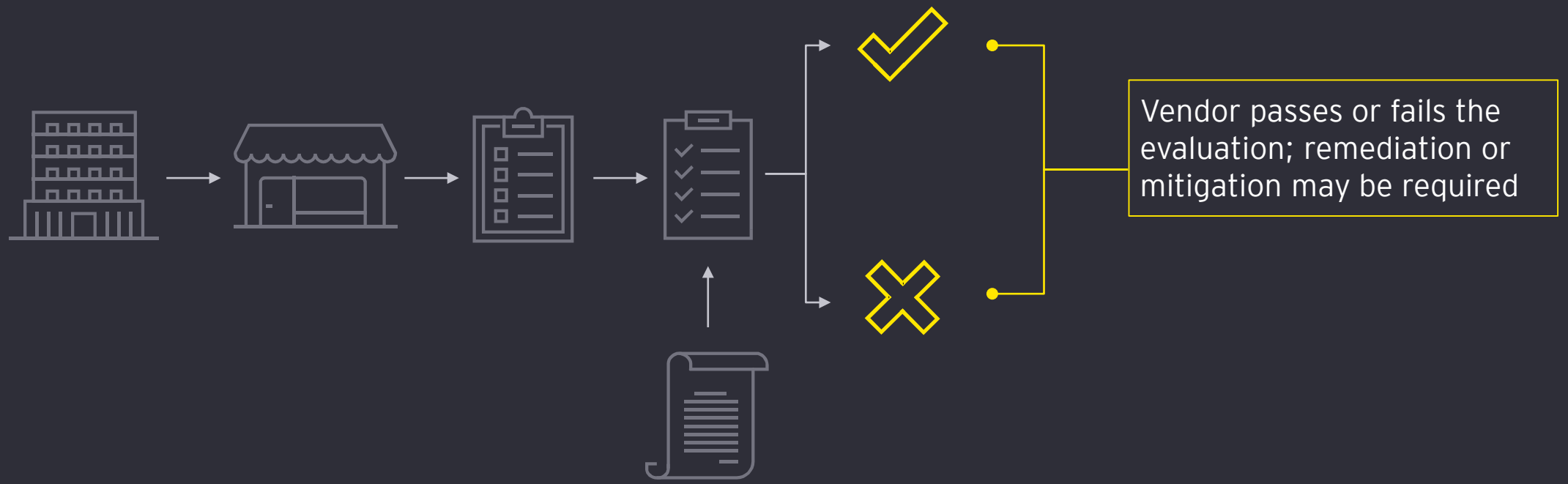
4

5

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

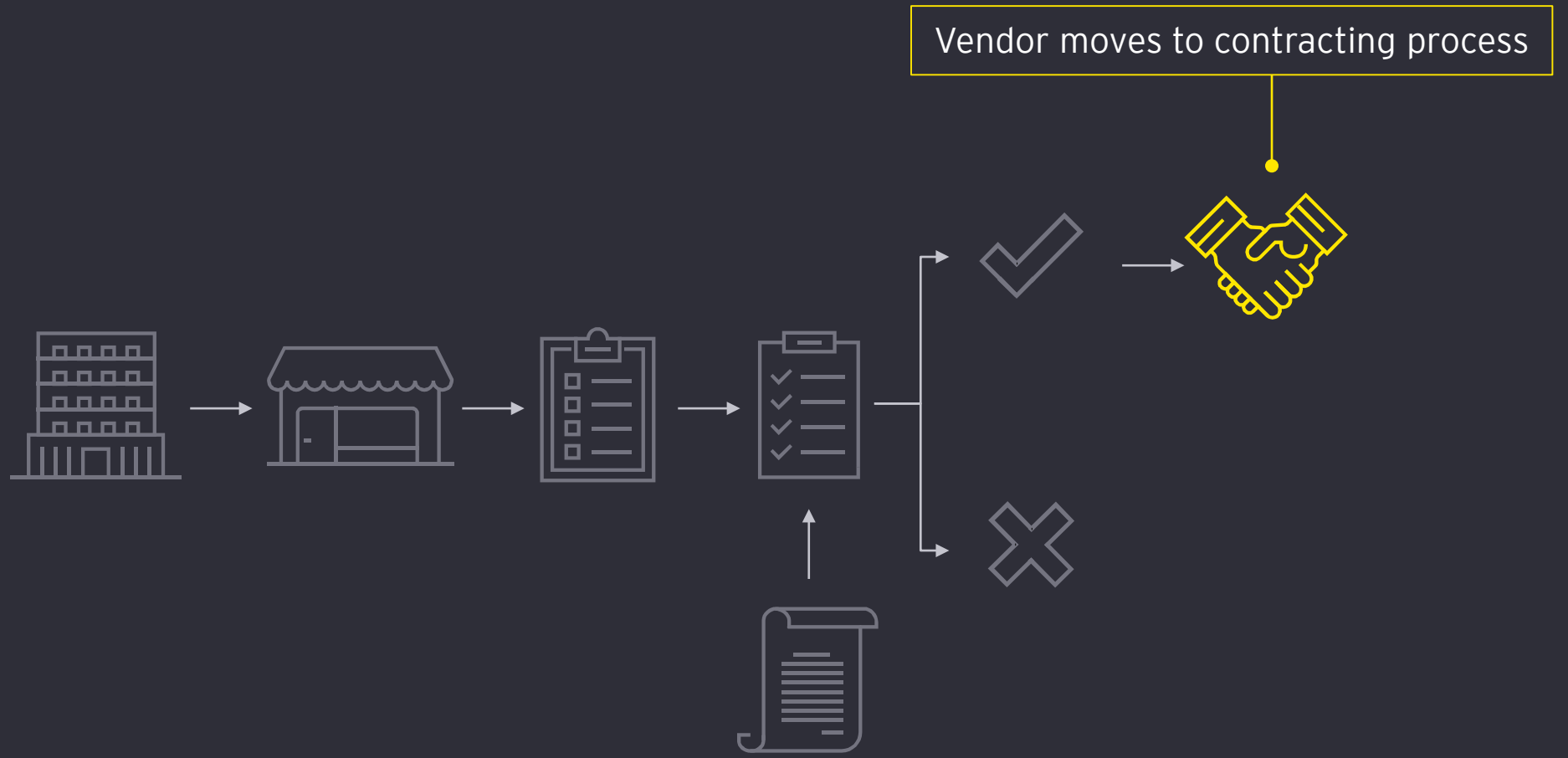
Traditional third-party risk management programs do not protect against supply chain attacks

1
2
3
4
5

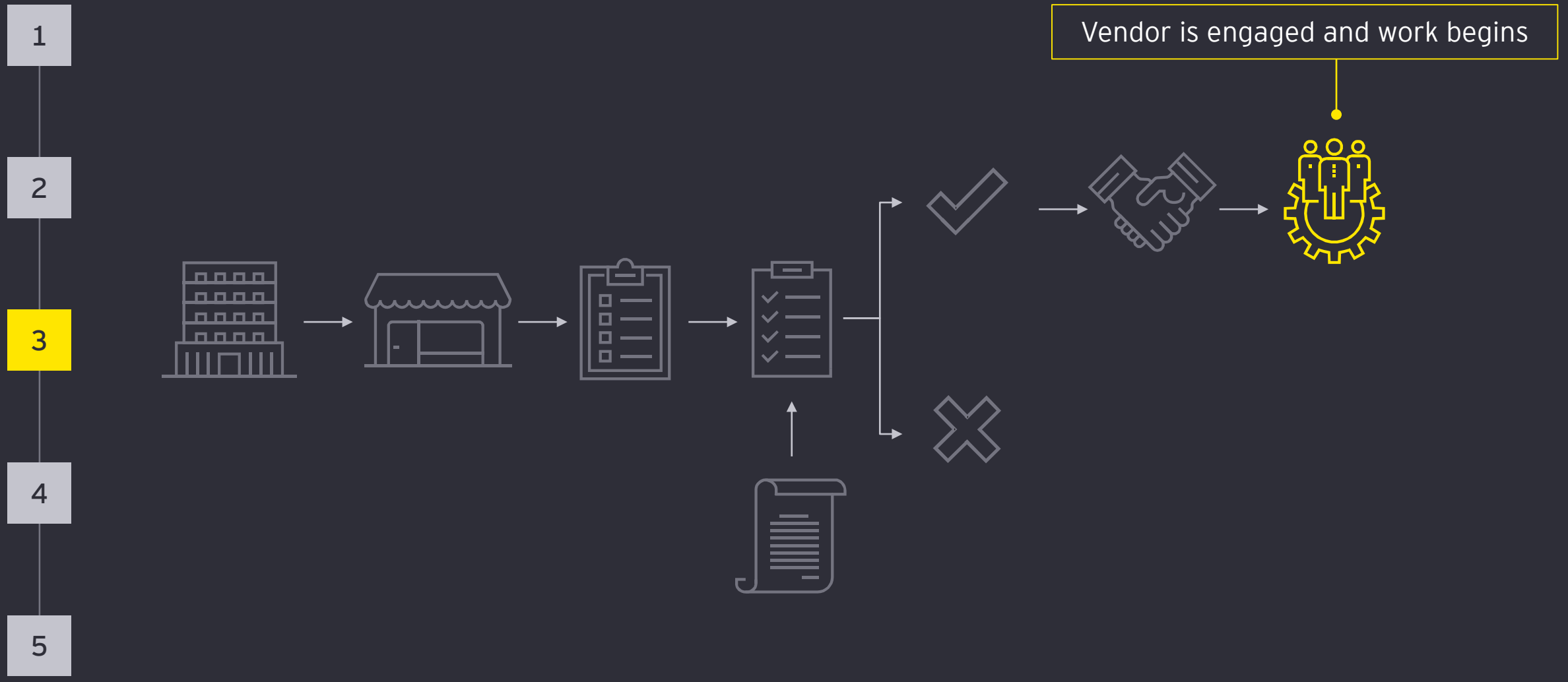


Traditional third-party risk management programs do not protect against supply chain attacks

1
2
3
4
5

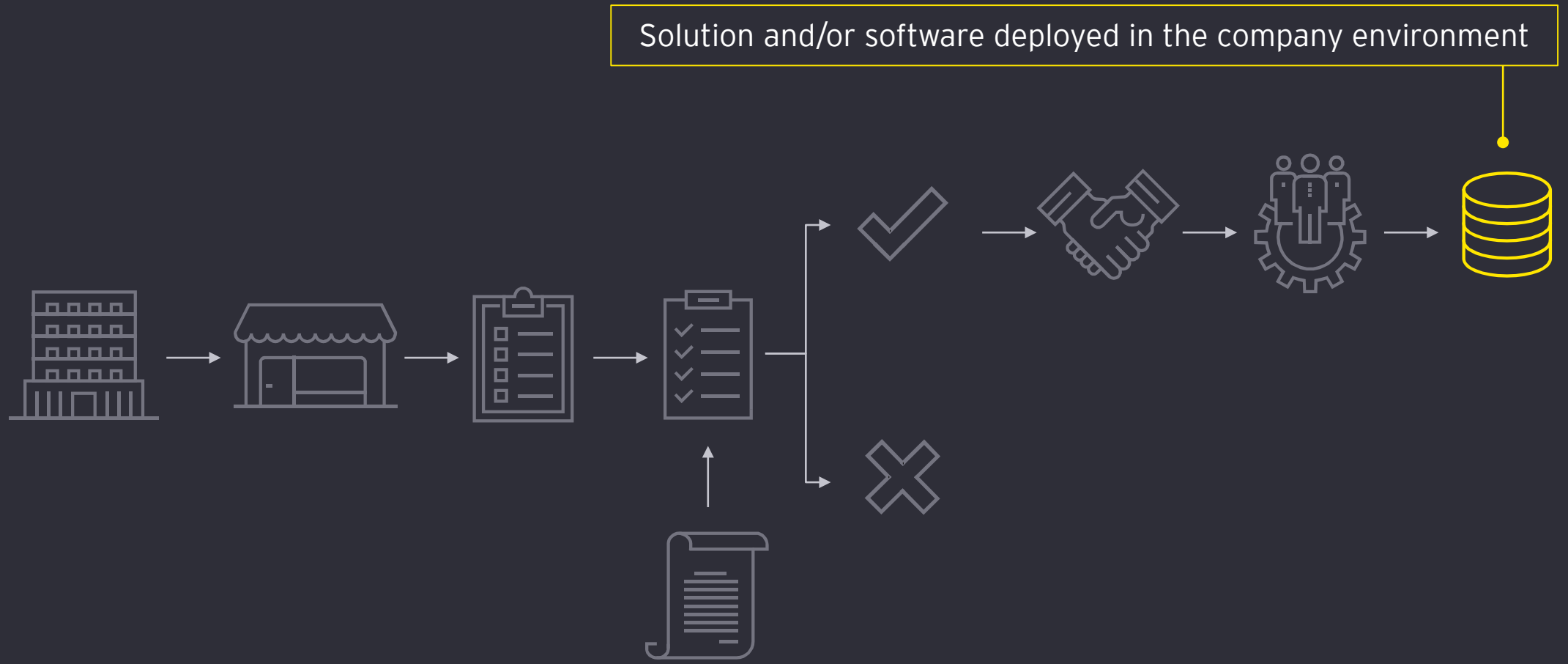


Traditional third-party risk management programs do not protect against supply chain attacks



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

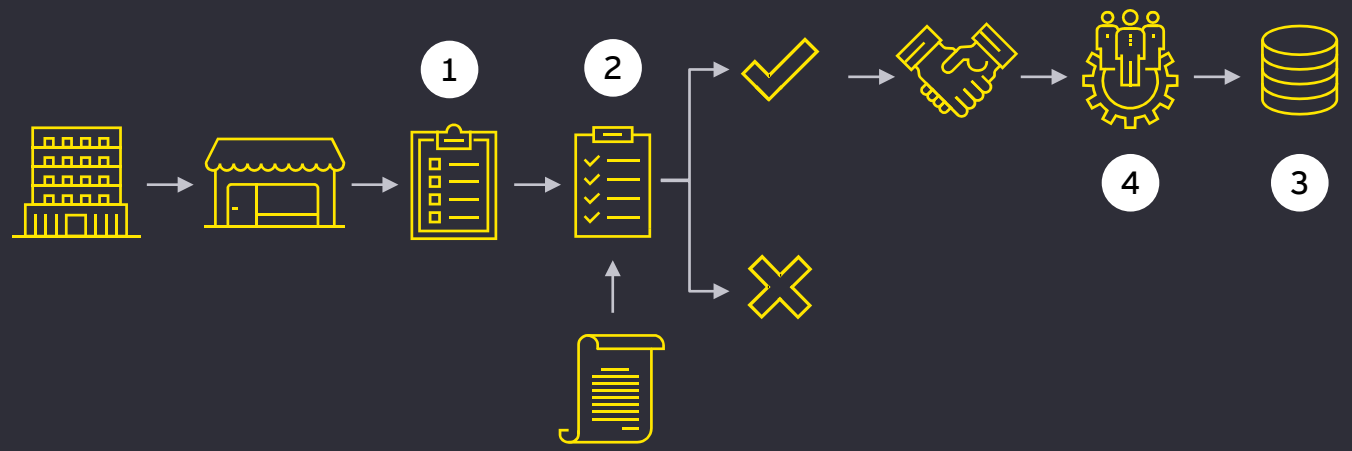
1
2
3
4
5



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

1
2
3
4
5

1. Questionnaires and certifications do not equal 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



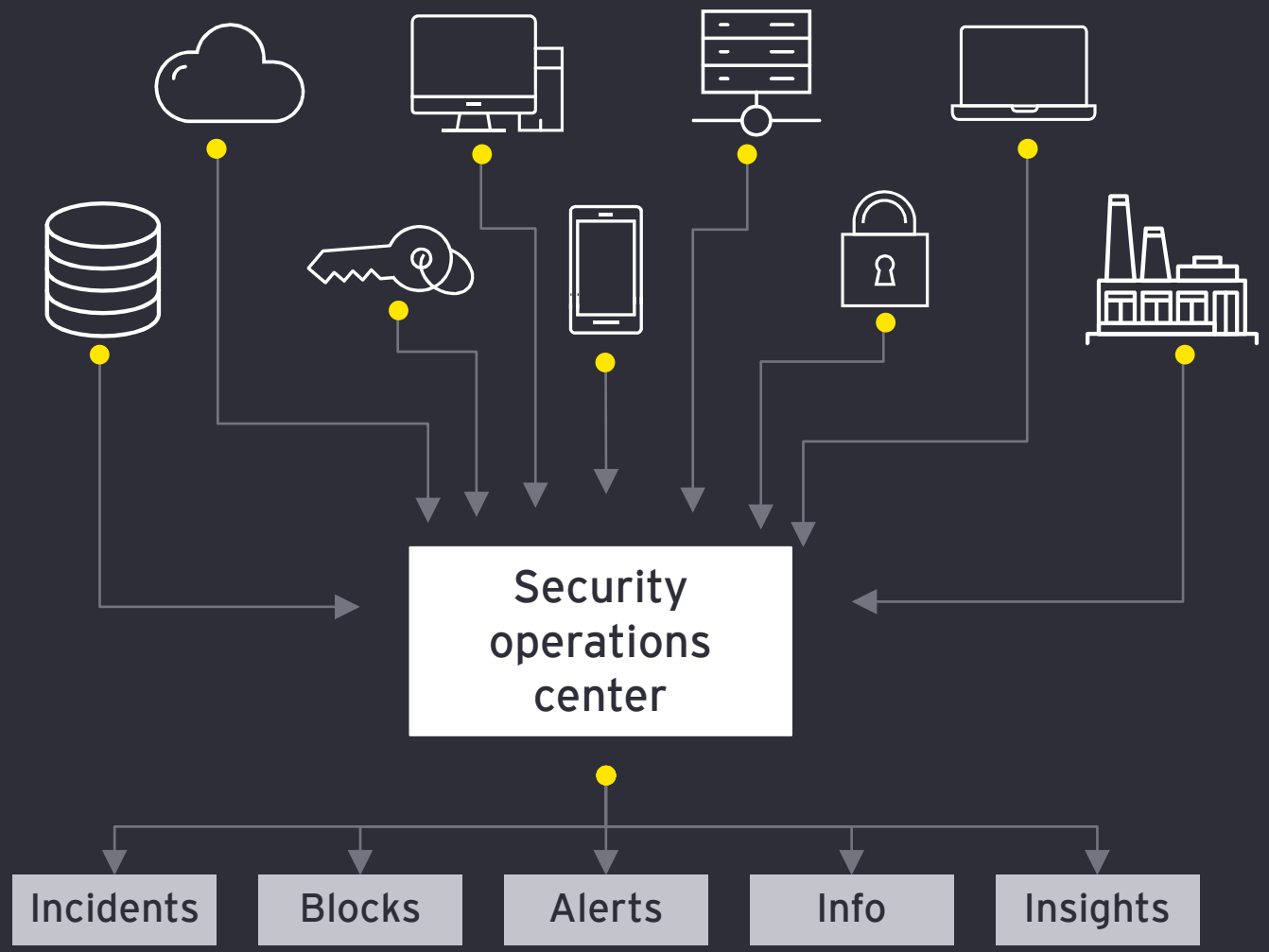
Third-party security risk management basic hygiene checklist

- ✓ 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

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 qualification and investigation
- SOC playbook and communication protocols
- Level 3 hand-offs, especially for MSSPs
- Automation versus manual processes; get ready for huge increase in volume

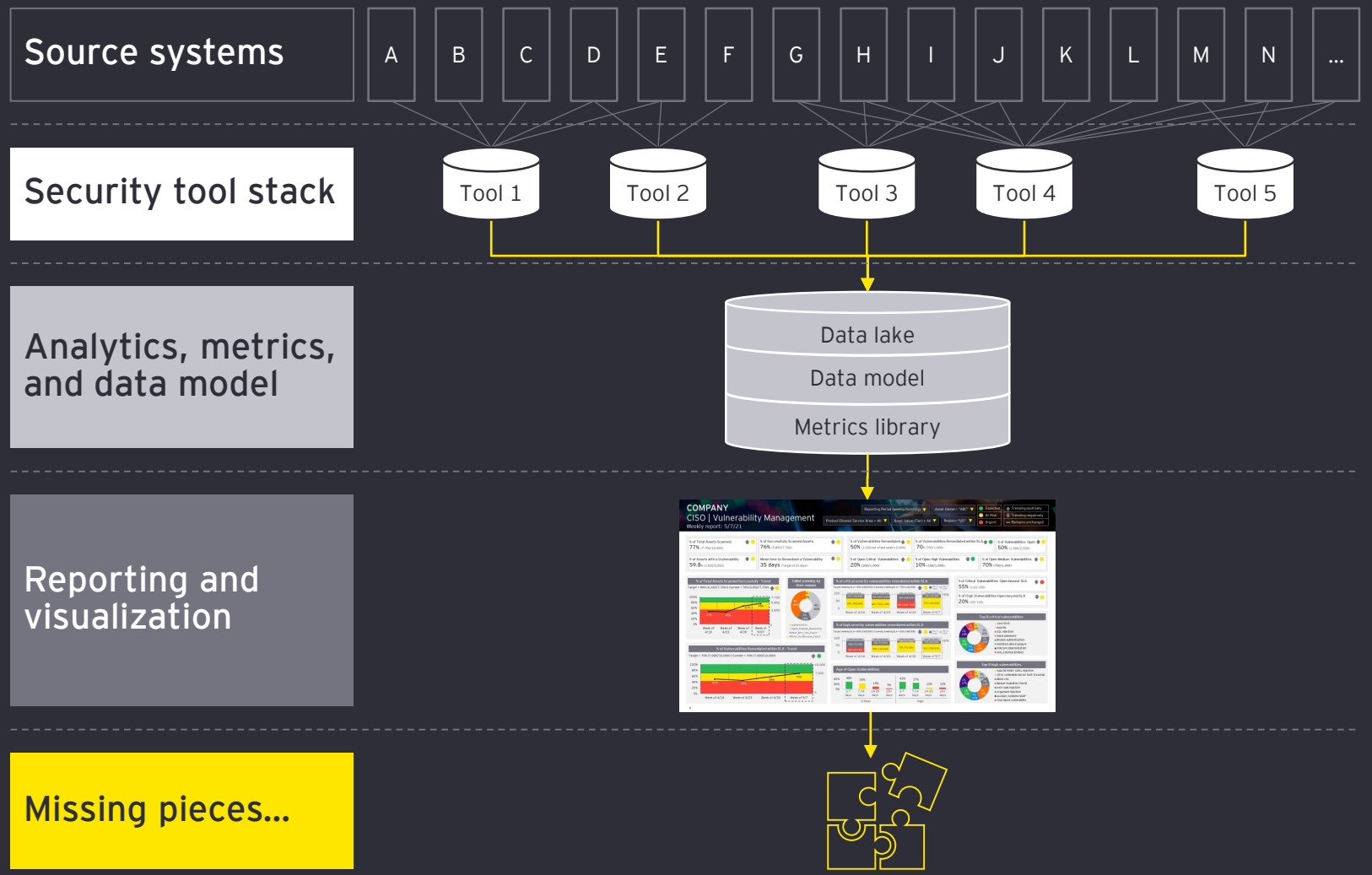


Cyber reporting, metrics and dashboarding are missing some critical elements before it can elevate cyber maturity

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 Cybersecurity Maturity Model Certification (CMMC) update

CMMC update

The Department of Defense (DoD) CMMC program was initiated in an effort to stop the erosion of US defense capabilities caused by the exfiltration of information from contractor networks.

CMMC

CMMC will require any contractor bidding to work on a DoD contract to first undergo an assessment by an independent third-party organization to verify that certain cybersecurity standards are met.

CMMC is an attempt by the DoD to standardize, validate and enforce cybersecurity practices, which is a shift from the self-attestation model currently utilized under DFARS (Defense Federal Acquisition Regulation Supplement) 252.204-7012.

It is likely that this requirement will impact more than 300,000 companies and that noncompliance with CMMC could threaten these organizations' ability to qualify for DoD contracts going forward.

Scope and applicability

- Non-federal entities (industry, academia, state, local and tribal governments)
- Controlled Unclassified Information (CUI) – information the government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls

Complying with regulatory requirements

- Projected timeline of the CMMC program rollout:
  - DoD is planning to roll out CMMC over the next five years with the goal of having 300k+ contractors certified by 2025.

DoD candidate programs (15 December 2020)

- Army
- Navy
- Air Force
- Missile Defense Agency

Preparing for the future

- CMMC maturity levels:
- Level 5 – advance/progressive
- Level 4 – proactive
- Level 3 – good cyber hygiene (SP 800-171)
- Level 2 – intermediate cyber hygiene
- Level 1 – basic cyber hygiene

CMMC compliance considerations

- Reciprocity with other US Government regulatory frameworks (i.e., FedRAMP)
- Control deficiency expectations
- Development of a System Security Plan (SSP)

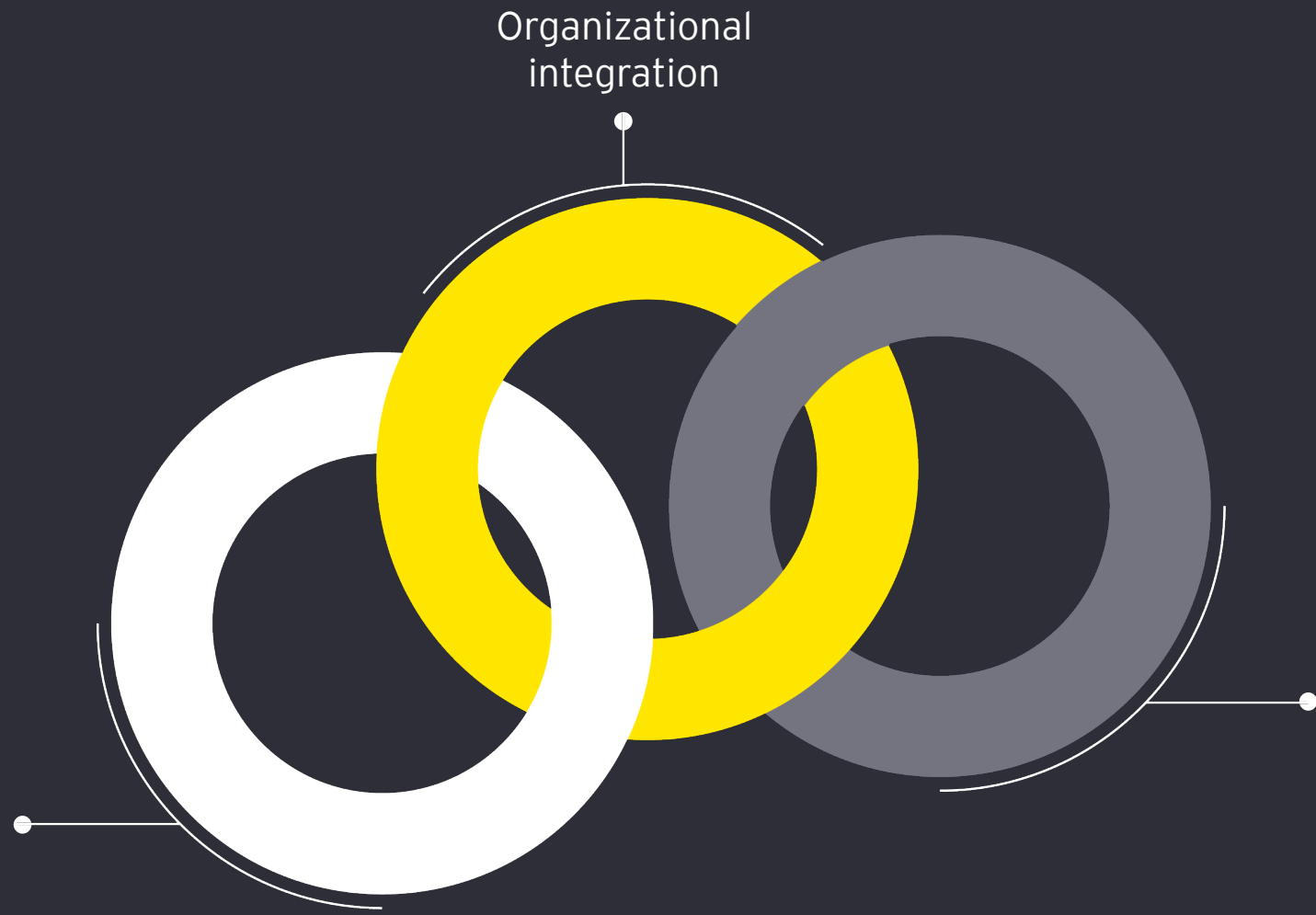
Supporting our national security

The DOD CMMC program was initiated in an effort to stop the erosion US defense capabilities caused by the exfiltration from contractor networks.

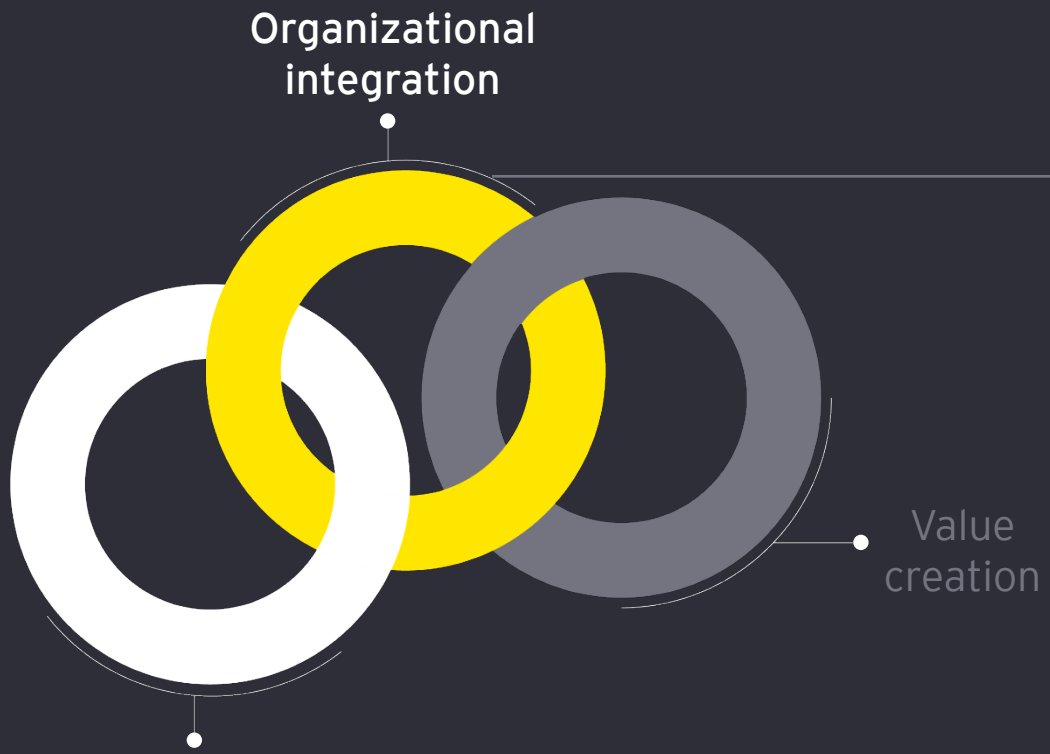
- "Industrial security scored the lowest among the eight dimensions with a 63 for 2019. In fact, industrial security has gained prominence as massive data breaches and brazen acts of economic espionage by state and non-state actors plague defense contractor in recent years."
- "The trend for cyber vulnerabilities indicates a tremendous change for the worse in global cybersecurity conditions."
- "DoD's demand for defense goods and services has trended sharply upward since 2017."

Vital Signs 2020: The Health and Readiness of the Defense Industrial Base, National Defense Industrial Association (NDIA)

Converting CMMC challenges into opportunities



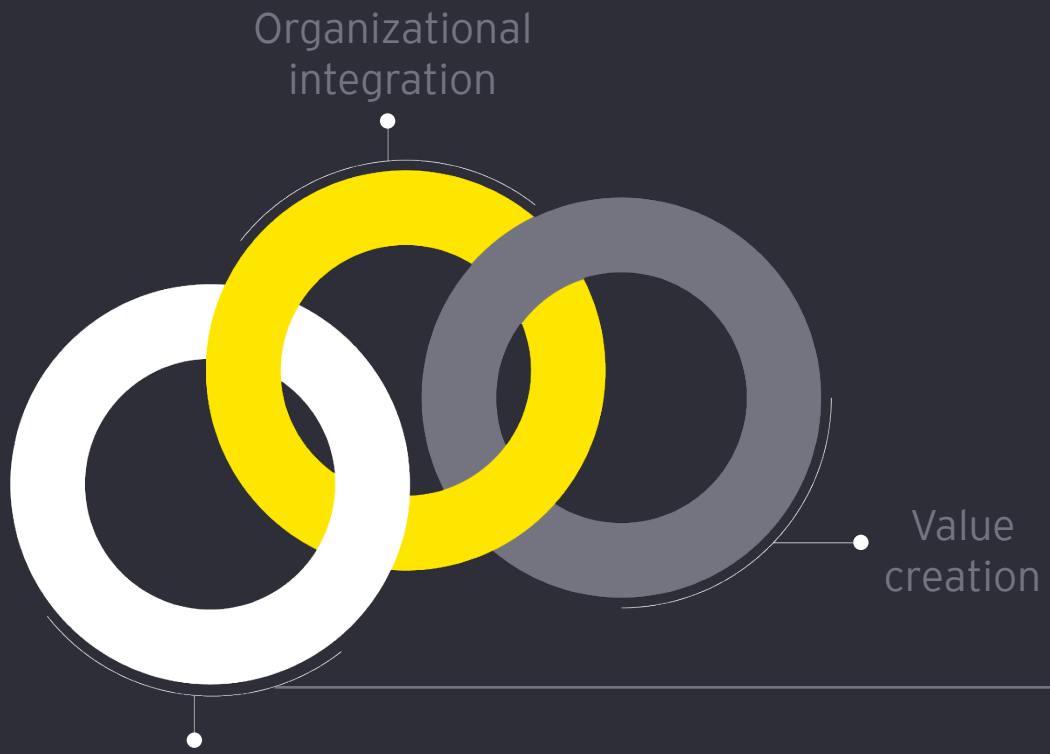
Converting CMMC challenges into opportunities



CMMC steering committee

- Chief executive officer
- Chief operating officer
- Chief growth officer
- Chief information officer
- Chief information security officer
- Chief risk officer
- Internal audit
- General counsel
- Procurement

Converting CMMC challenges into opportunities



People

- Develop workforce of the future
- Integrate internal and external stakeholders

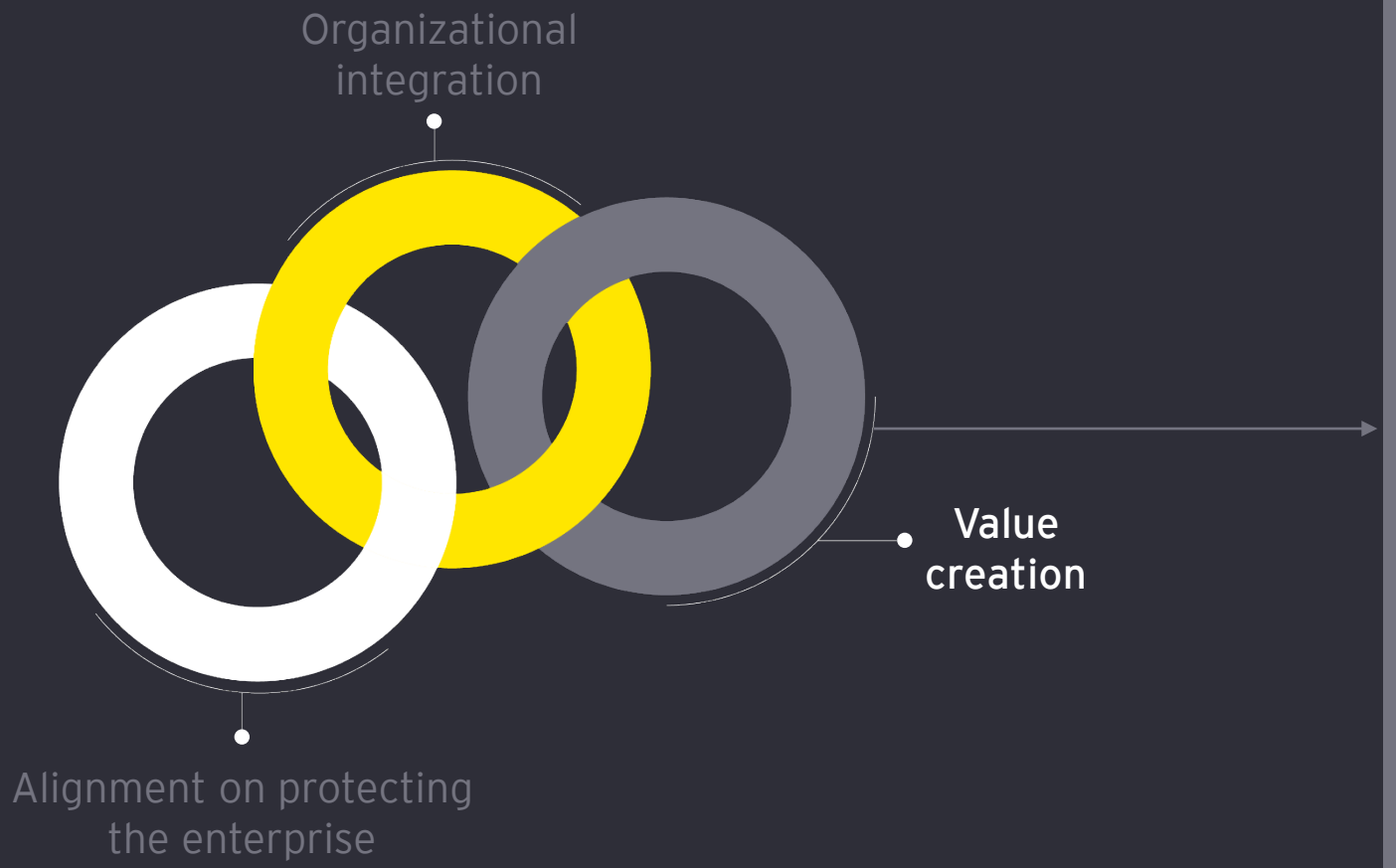
Process

- Optimize enterprise-wide protection
- Integrate people and data

Technology

- Enable high value data protection
- Enable governance risk and compliance

Converting CMMC challenges into opportunities



Risk reduction and operational efficiencies

- Unified and clear vision of stakeholder expectations
- Informed decision-makers across the organization
- Organization growth potential with existing or new potential clients
- Comprehensive understanding of services being provided to the US government
- Improvement in quality of risk information and data availability for decision-making
- Single point of truth for critical risk management matters
- Increased confidence with cyber maturity and investments

EY CMMC and Cyber thought leadership

What should be top on mind to continue preparing for CMMC:

Click here

Over the past few months, the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) and the Department of Defense (DoD) have been very active with the implementation of the Cybersecurity Maturity Model Certification (CMMC). They have agreed on a no-cost contract, released the interim rule and revealed the initial pathfinder contracts. All this came amid news of major cybersecurity breaches, which heightened the DoD's need to continue making cybersecurity a priority.

Cybersecurity Maturity Model Certification officially becomes part of DFARS

The DoD's interim rule of September 29, 2020, *Assessing Contractor Implementation of Cybersecurity Requirements* (DFARS Case 2019-D041), has been effective since November 30, 2020. The interim rule laid the foundation for implementing the CMMC and detailed the DoD's phased rollout of CMMC assessment requirements through September 30, 2025. As part of the interim rule, the DoD surprised contractors with a requirement that they perform a self-assessment of their cybersecurity compliance. The assessment focused on the National Institute of Standards and Technology Special Publication (NIST SP) 800-171 security controls, which are the same controls required of contractors as part of the DFARS 252.204-7012 clause.

The new rule included the following new DFARS provision and clause, which will start appearing in DoD specified solicitations and contracts moving forward:

1. DFARS Provision 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements as prescribed by DFARS 204.7304 (d)

   The provision requires contractors to have a current (not older than three years) assessment score in the Supplier Performance Risk System (SPRS) before an award. As part of the entry into SPRS, contractors are to include system security plan name, CAGE code, a brief description of plan architecture, the date of the assessment, total score and the date that all controls will be implemented (if not already fully implemented).

2. DFARS Clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements as prescribed by DFARS 204.7304 (e)

   The clause defines the types of assessments (basic, medium, high) and the methodology. It also clarifies that for a basic assessment, contractors are to perform a self-assessment and enter their score in SPRS. For medium and high assessments, personnel from the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) would perform the assessment using NIST SP 800-171A. With the basic assessments reported in SPRS, the DoD will be able to understand the contractor's current levels of compliance without undertaking intensive reviews of contract or program-specific reviews.

3. DFARS Clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements as prescribed by DFARS 204.7503 (a)(b)

   When included in solicitations, the clause will require contractors to achieve the CMMC certification at the time of the award at the level specified in the solicitation and will have to maintain that certificate for the life of the contract, task, or delivery order.

Busy end to 2020 for CMMC

December 2020 proved to be eventful for CMMC with the release of the assessment guides and announcement of the initial pathfinder contracts. The CMMC-AB released the assessment guides for Level 1 and Level 2 certification. While the assessment guides leverage the NIST SP 800-171A on assessing the 110 controls from NIST SP 800-171, the Level 3 guide provided answers on how the additional 20 controls for Level 3 CMMC will be assessed.

With these guides, contractors now have direction on how they will be evaluated and DoD's expectations. There was also insight on what to expect with the pathfinder contracts announcement. In particular, the DoD identified seven contracts expected to serve as experiments for CMMC in 2021. Here are the contracts for the Navy, Air Force and Missile Defense Agency:

Navy	Air Force	Missile Defense Agency
• Integrated Common Processor • Flt-18E/F Full Mod of the SB&R and Shut-off Valve • Vent services for the Arleigh Burke Class destroyer	• Mobility Air Force Tactical Data Links • Consolidated Broadband Global Area Network Follow-On • Azure Cloud Solution	• Technical Advisory and Assistance Contract

What does this mean for contractors?

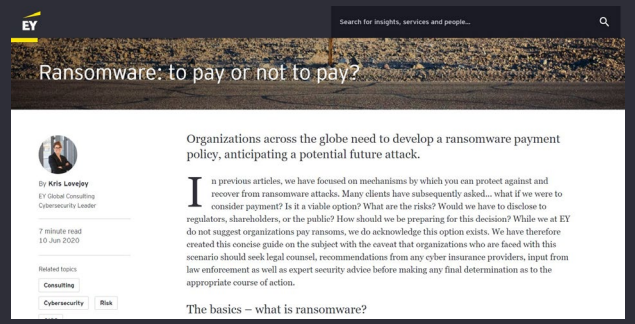
While many of these developments merely formalized what contractors were expecting, there is a lot for DoD contractors to digest and implement. Here are key actions and considerations contractors should consider:

- To be eligible for future awards, contractors must first perform a self-assessment against NIST SP 800-171 requirements using the DoD assessment methodology and enter their score in SPRS. Any outstanding POA&Ms (Plans of Action and Milestones) items identified during the assessment will no longer be able to have an indeterminable closure period as contractors will need to describe the plan to achieve 100% compliance with NIST SP 800-171 requirements.
- The DoD assessment methodology provided to contractors for their self-assessment has a maximum score of 110 (1 point for each implemented control). A negative score is possible since certain controls can be assigned more than one point, which would be deducted if the control is not in place.
- In addition to applying to contractors who serve as a prime to the US government, the requirements also apply to subcontractors on contracts that include the contract clauses identified previously. The prime contractor still have the responsibility to verify that the subcontractor is compliant. If a subcontractor is unable to achieve compliance, primes may need to evaluate whether other subcontractors that are compliant can perform the same work. Additionally, subcontractors should keep in mind that, while they may not process, store or transmit controlled unclassified information, they still must obtain a CMMC Level 1 certification to serve as a subcontractor.
- Contractors should be mindful that the government reserves the right to perform random audits to confirm that contractors properly self-assess and accurately score themselves. DCMA also will check on whether an SSP (System Security Plan) exists and that the contractor is progressing towards their POA&Ms.

Cybersecurity Maturity Model Certification: top of mind | 6

What to do when faced with ransomware:

Click here



Search for insights, services and people...

Ransomware: to pay or not to pay?

By **Kris Lovejoy**
EY Global Consulting Cybersecurity Leader

7 minute read
10 Jun 2020

Related topics
Consulting
Cybersecurity
Risk

Organizations across the globe need to develop a ransomware payment policy, anticipating a potential future attack.

In previous articles, we have focused on mechanisms by which you can protect against and recover from ransomware attacks. Many clients have subsequently asked... what if we were to consider payment? Is it a viable option? What are the risks? Would we have to disclose to regulators, shareholders, or the public? How should we be preparing for this decision? While we at EY do not suggest organizations pay ransoms, we do acknowledge this option exists. We have therefore created this concise guide on the subject with the caveat that organizations who are faced with this scenario should seek legal counsel, recommendations from any cyber insurance providers, input from law enforcement as well as expert security advice before making any final determination as to the appropriate course of action.

The basics – what is ransomware?

4 Questions and answers

THANK YOU

Justin Greis

Michael Hinckley

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.

2105-3779053
ED None

ey.com