Crowe

Get clarity on what’s ahead

Crowe 2020 Financial Services Conference

(CYBER) RISK AND UNCERTAINTIES

SMART DECISIONS. LASTING VALUE.™

HOUSEKEEPING AND CPE

PLEASE NOTE:

- All of today’s audio is being broadcast to your computer speaker.
- Please submit questions through the Q&A function on your screen. Questions will be addressed at the end of the presentation.
- To download a copy of the presentation or access the resources connected to this session, please visit the resources icon at the bottom of your console.

CPE CREDIT

- Log in individually to the session
- Successfully complete 3 of the 4 attendance checks or polling questions

NO CPE CREDIT

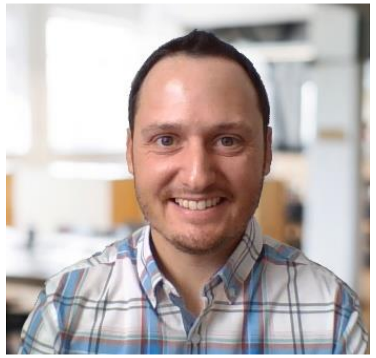
- Fail to successfully complete 3 of the 4 attendance checks
- Viewing a recording of this session (CPE is only awarded for live sessions)

CPE CERTIFICATE OF COMPLETION

Will be e-mailed within two weeks of successfully passing this program

Upon completion of this program you will receive post event evaluation.

YOUR PRESENTER



Dave McKnight, CISSP

Principal

Bachelor of Science, Information Technology
Rochester Institute of Technology
Rochester, New York

Certified Information Systems Security Professional (CISSP)

Epic Systems 2014 and 2016 Security Coordinator Certified

Profile

Dave McKnight works with mid-sized financial services organizations to refine their cybersecurity capabilities. He is a Principal at Crowe LLP and co-leads Crowe's Digital Security for Financial Services practice.

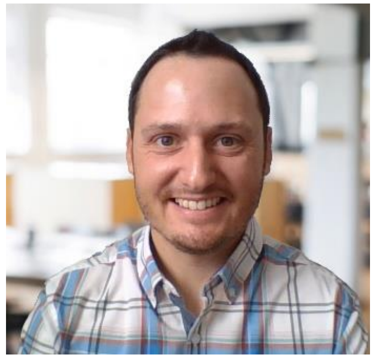
Over twenty years of Information Security experience; sixteen years of focused penetration testing, security assessing, and IT incident and forensics specialization.

Previous manager of Crowe's in-house information security focused training curriculum that is utilized throughout the year to train our Cybersecurity professionals.

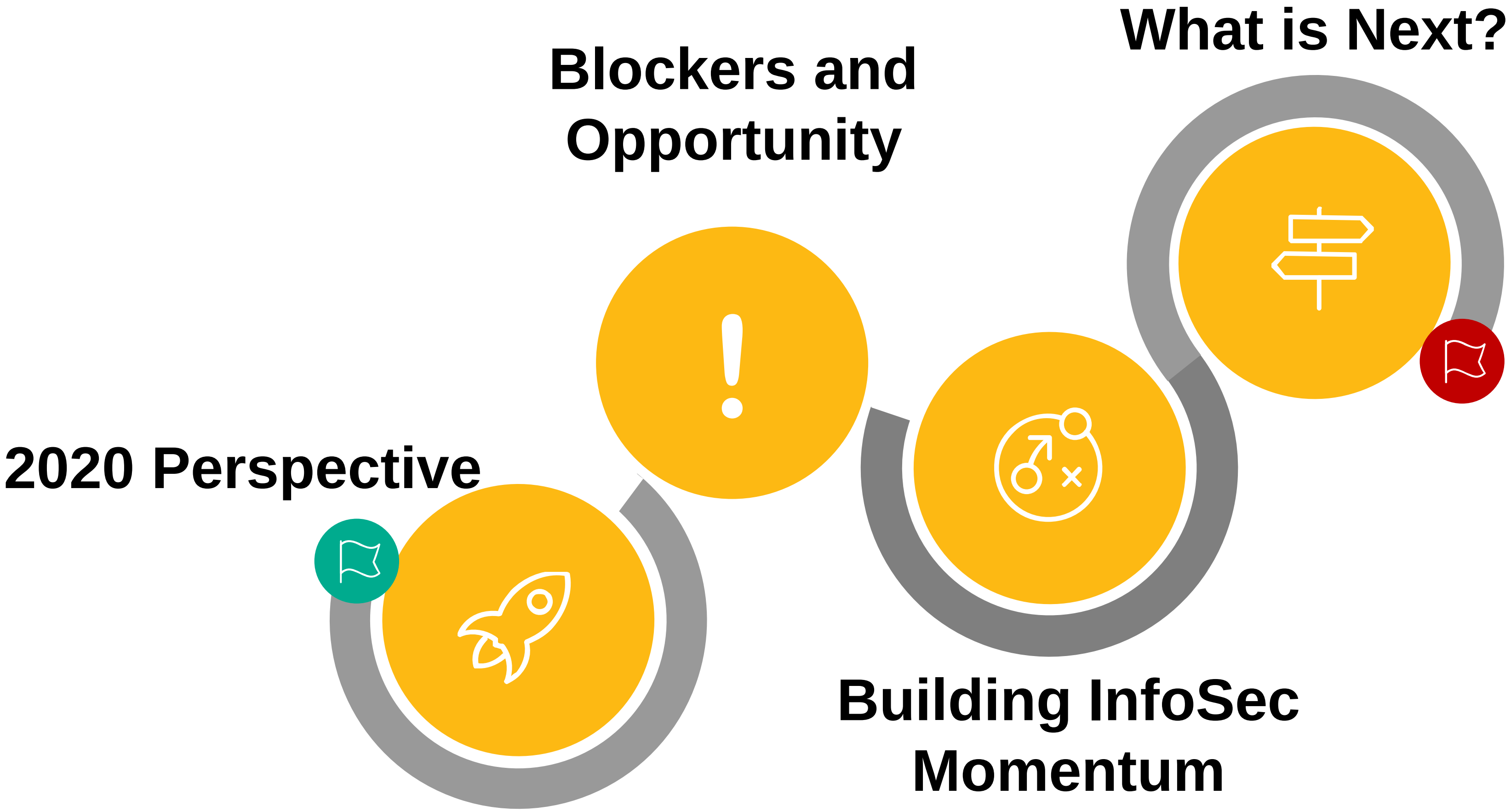
Publications and Speaking Engagements

- Speaker, "Navigating the Security Risks of Rapidly Going Remote", 2020 ABA
- Publication, "5 Global Cyberthreats – and How to Fight Them", 2019 Forbes
- Speaker, "Leveraging Cybersecurity to Drive Organizational Growth" 2019 Corporate Financial Reporting Insights Conference
- Publication, "Building and Maintaining Momentum in Bank Cybersecurity", 2019 Crowe Banking Performance Insights
- Speaker, "Achieving a Cybersecure Organization", 2018 IIA Financial Services Audit Center
- Publication, "One Year Later: Cybersecurity Practices Shift After the Equifax Breach", 2018 BankNews

YOUR PRESENTER



Dave McKnight, CISSP
Principal



Accommodating, Adjusting, Accelerating

Banks have (mostly) modified their existing infrastructure, supported platforms, and communications.

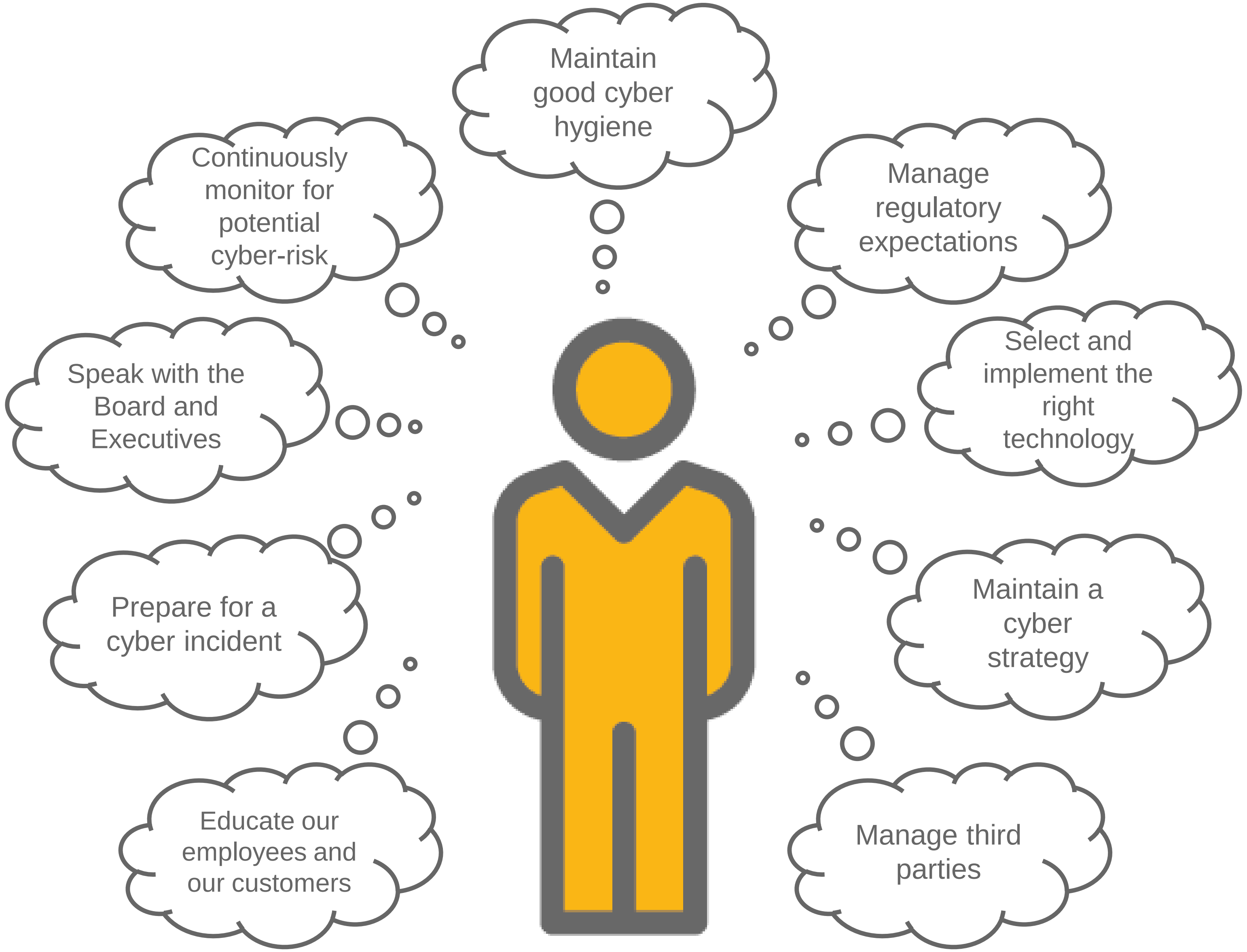
Accommodating, Adjusting, Accelerating

Banks have (mostly) modified their existing infrastructure, supported platforms, and communications.

Deeper Technology Considerations across Risk Management

Banks are evaluating specific risk’s, associated with their usage of technology, storage of electronic data, and partnerships with third-parties.

On the Minds of our CISOs



Maintain good cyber hygiene
Continuously monitor for potential cyber-risk
Manage regulatory expectations
Speak with the Board and Executives
Select and implement the right technology
Prepare for a cyber incident
Maintain a cyber strategy
Educate our employees and our customers
Manage third parties

On the Minds of our CISOs

2020 Cyber fraud and abuse

20%

71% of breaches were financially motivated and **25%** were motivated by espionage.

The **average lifecycle** of a breach lasted almost **11 MONTHS**

(breach → containment)

Half of breaches featured hacking, **28%** involved malware and **32–33%** included phishing or social engineering, respectively.

Retrieved from: https://enterprise.verizon.com/en-gb/resources/reports/dbir/, https://www.arkoselabs.com/, https://www.ibm.com/security/data-breach

Poll

How much has your mobile workforce expanded throughout 2020?

A. Less than 25%

B. Between 25%-50%

C. Between 50%-100%

D. More than 100%

E. Unsure

2020 Perspective

Our People

Deployment and expansion of our IT connectivity, such as **Microsoft365, Virtual Private Networks, Bring Your Own Device**

2020 Perspective

Our People

Deployment and expansion of our IT connectivity, such as **Microsoft365, Virtual Private Networks, Bring Your Own Device**

Operations

Continuing on-going **Digital Transformation,** adjustments to budgets, personnel changes and challenges.

2020 Perspective

Our People

Deployment and expansion of our IT connectivity, such as **Microsoft365, Virtual Private Networks, Bring Your Own Device**

Our Customers

Those whom continue to bank in-person vs. those whom desire a robust virtual experience.

Operations

Continuing on-going **Digital Transformation,** adjustments to budgets, personnel changes and challenges.

2020 Perspective

Our People

Deployment and expansion of our IT connectivity, such as **Microsoft365, Virtual Private Networks, Bring Your Own Device**

Our Customers

Those whom continue to bank in-person vs. those whom desire a robust virtual experience.

Operations

Continuing on-going **Digital Transformation,** adjustments to budgets, personnel changes and challenges.

Risk and Regulation

Social engineering attacks (vishing and phishing) have risen. **Successful attacks are growing more impactful and costly**. Audits and examination visits are requiring “more” resources and have higher expectations.

Blockers and Opportunity

Blockers and Opportunity

- Staying productive and maintaining confidentiality (while virtual)

- Maintaining connectivity to our employees and customers (secure and consistent connectivity)

Blockers and Opportunity

- Staying productive and maintaining confidentiality (while virtual)
- Understanding and demonstrating conformance to organizational policies and procedures

- Maintaining connectivity to our employees and customers (secure and consistent connectivity)
- Validating, adjusting, and communicating policies and procedures related to usage of technology, protection of data, and security awareness

Blockers and Opportunity

- Staying productive and maintaining confidentiality (while virtual)
- Understanding and demonstrating conformance to organizational policies and procedures
- Responding to increased operational needs with reductions in operational resources

- Maintaining connectivity to our employees and customers (secure and consistent connectivity)
- Validating, adjusting, and communicating policies and procedures related to usage of technology, protection of data, and security awareness
- Consider automation and elimination of duplicative or overlapping tasks

Poll

Are you allowing your now-mobile workforce to use personal devices for work purposes?

A. Yes

B. No

C. Unsure

Keys to a stronger Cybersecurity Program

Knowing what you are attempting to protect.
(Asset Identification and Management)

Keys to a stronger Cybersecurity Program

Knowing what you are attempting to protect.
(Asset Identification and Management)

Tailoring your Information Security Program and Risk Management to your assets.

Keys to a stronger Cybersecurity Program

Knowing what you are attempting to protect.
(Asset Identification and Management)

Tailoring your Information Security Program and Risk Management to your assets.

Striving for continuous improvement of your cyber hygiene.

Keys to a stronger Cybersecurity Program

Knowing what you are attempting to protect.
(Asset Identification and Management)

Tailoring your Information Security Program and Risk Management to your assets.

Striving for continuous improvement of your cyber hygiene.

Be inclusive of all employees when it comes to cybersecurity.

Keys to a stronger Cybersecurity Program

Knowing what you are attempting to protect.
(Asset Identification and Management)

Tailoring your Information Security Program and Risk Management to your assets.

Striving for continuous improvement of your cyber hygiene.

Be inclusive of all employees when it comes to cybersecurity.

Intentionally **prepare** for a **cyber-event.**
(Threat modeling, breach simulations, table-top exercises)

Building Information Security Momentum

Utilize Known Frameworks

Rely on creditable and referenceable cybersecurity guidance and direction.

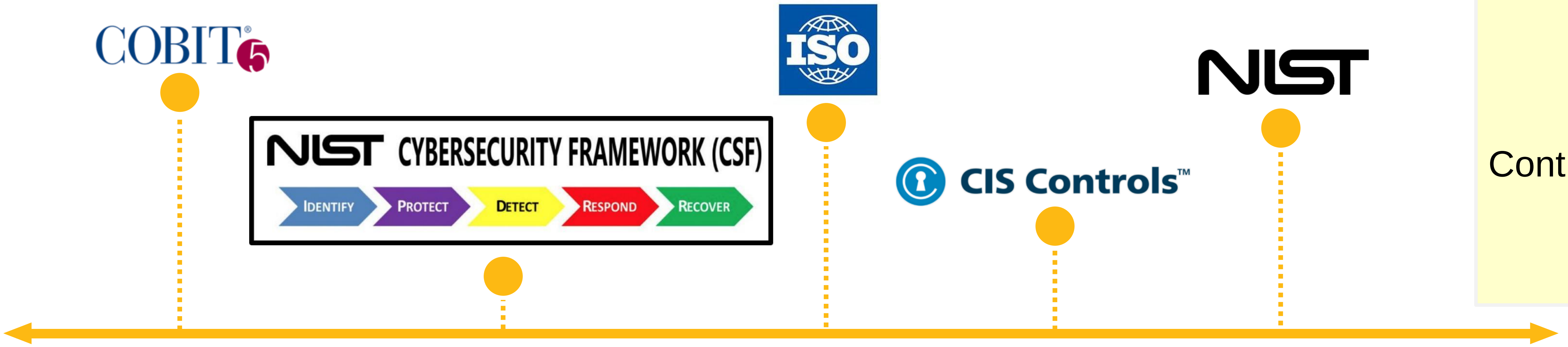
Control Expectation

VS

Control Expectation

VS

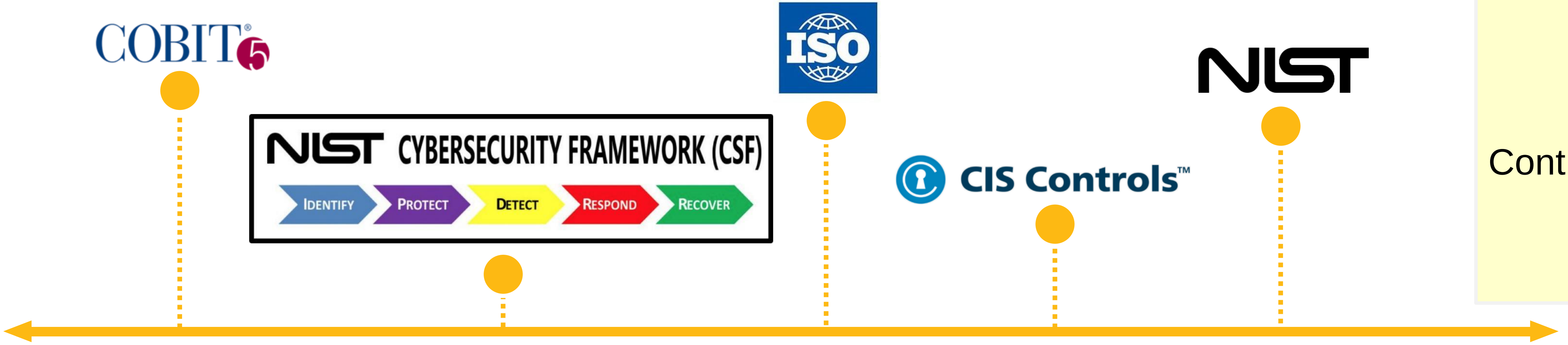
Control Maturity
& Risk Assessing



Control Expectation

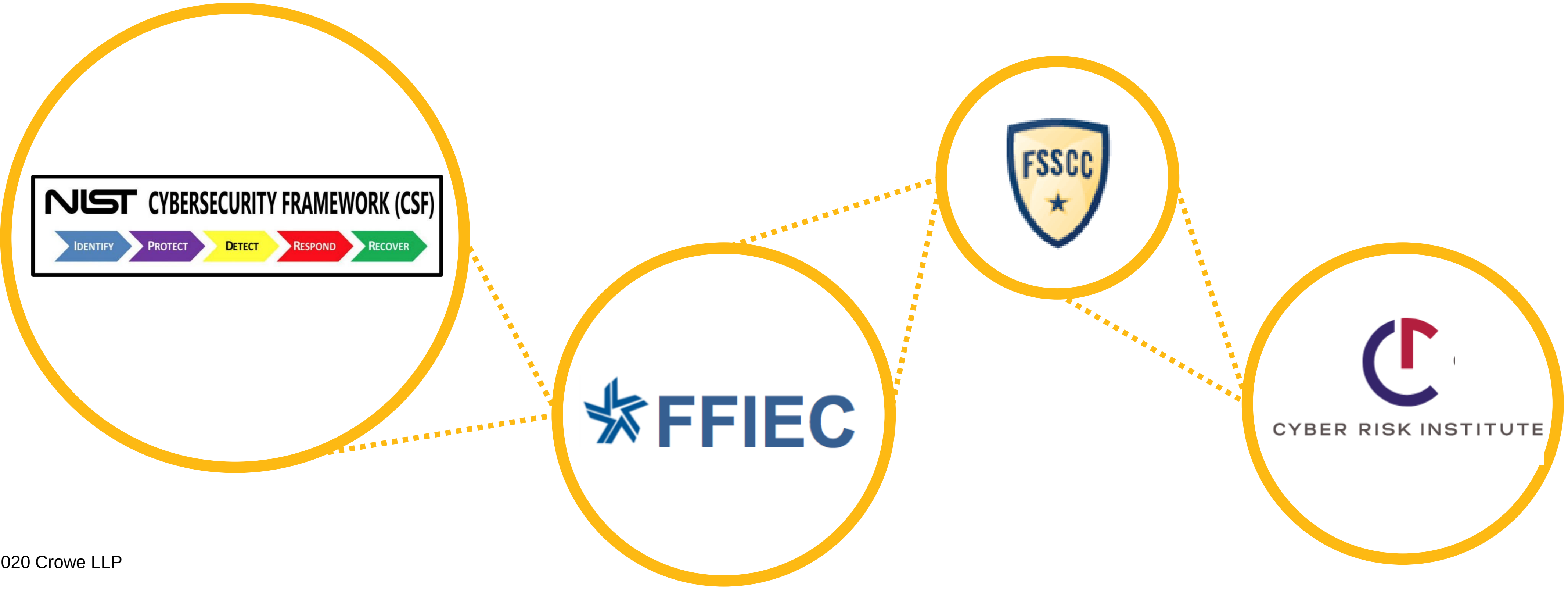
VS

Control Maturity
& Risk Assessing



Control Expectation

VS



Control Maturity
& Risk Assessing

Poll

What do you see as the most impactful cyber risk related to embracing remote workforces?

A. Malicious Threat Actors

B. Insecure or Less Secure Third Parties

C. Employee Errors

D. Lack of Secure Technologies

E. Unsure

Building Information Security Momentum

Utilize Known Frameworks

Rely on creditable and referenceable cybersecurity guidance and direction.

Understand Your Risks

Establish a Cybersecurity Risk Appetite Statement and Tolerance.

Cybersecurity Risk Appetite and Tolerances

Cyber Risk Appetite

“..the level of **tolerance** that an organization has for **risk**.”

RSA

Cyber Risk Appetite

“..the level of **tolerance** that an organization has for **risk**.”
RSA

“..the amount of **risk**, on a broad level, an organization is **willing to accept in pursuit of value.”**
COSO

Cyber Risk Appetite

“..the level of **tolerance** that an organization has for **risk**.”
RSA

“..the amount of **risk**, on a broad level, an organization is **willing to accept in pursuit of value.**”
COSO

“the **amount** and **type** of **risk** that an organization **is willing to take in order to meet their strategic objectives**”
Institute of Risk Management

A risk appetite frames the risk management process, optimizes business performance and helps meet stakeholder expectations.

Example: Community Bank

- ABC Bank’s appetite for cybersecurity risk is moderate.

- ABC Bank’s confidentiality, integrity, and availability of our assets is affected by cyber risk. Our assets are vital to maintain our business practices and therefore must be safeguarded from both external and internal threats, misuse, modification, and unintended damage. ABC Bank’s primary objective is to protect our assets to ensure the safety and soundness of our information systems. We will be successful through the utilization of appropriate internal controls, an cyber-aware workforce, governance, timely remediation of identified control weaknesses, and consistent third-party management.

Poll

Do you plan to maintain or expand your current mobile workforce in 2021?

A. Yes, completely or more than now

B. Yes, but at a reduce amount

C. No

D. Unsure

Building Information Security Momentum

Utilize Known Frameworks

Rely on creditable and referenceable cybersecurity guidance and direction.

Understand Your Risks

Establish a Cybersecurity Risk Appetite Statement and Tolerance.

Invest Where It Counts

Consider how your IT investments will better Operations, Customers, and your Business Strategy.

Always consider your Cyber Risk Tolerance.

“New” Tools

Cloud Technology

Zero Trust

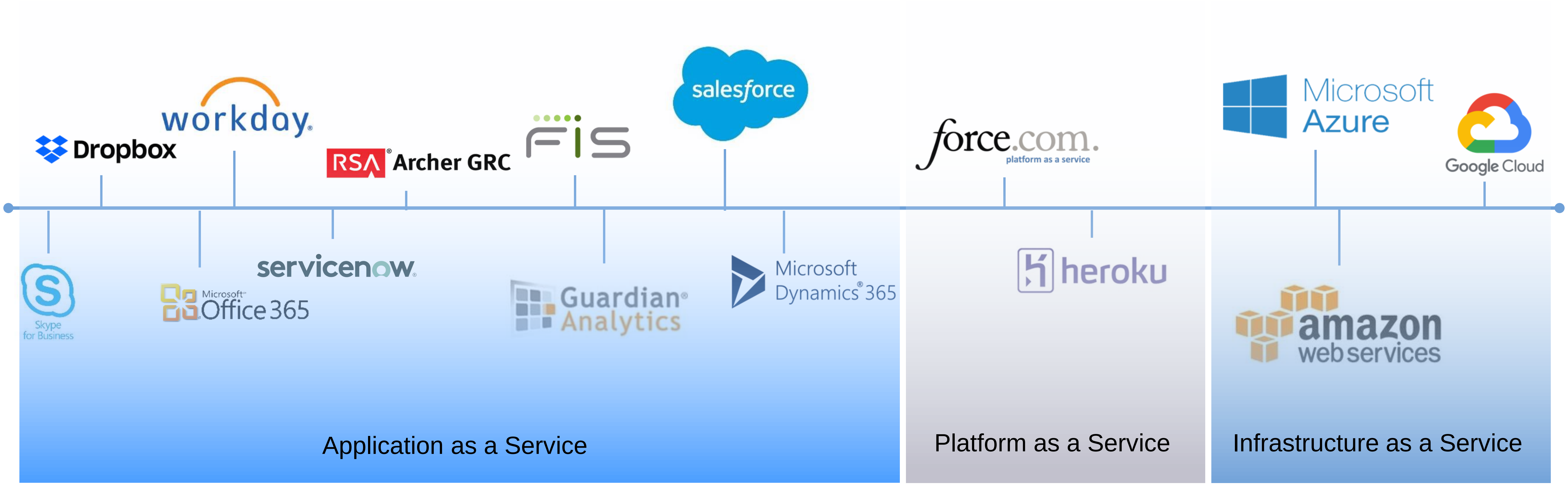
Risk Quantification

Why do organizations adopt cloud?

- Improved innovation and collaboration
- Faster development and speed to market
- Greater flexibility to adopt new technology
- Increased mobility and agility of workforce
- Growing customer product and platform options

- Reduced technology costs
- More robust security options
- Improved business continuity
- Smaller technology and environmental footprint

What the cloud is doing for financial institutions…

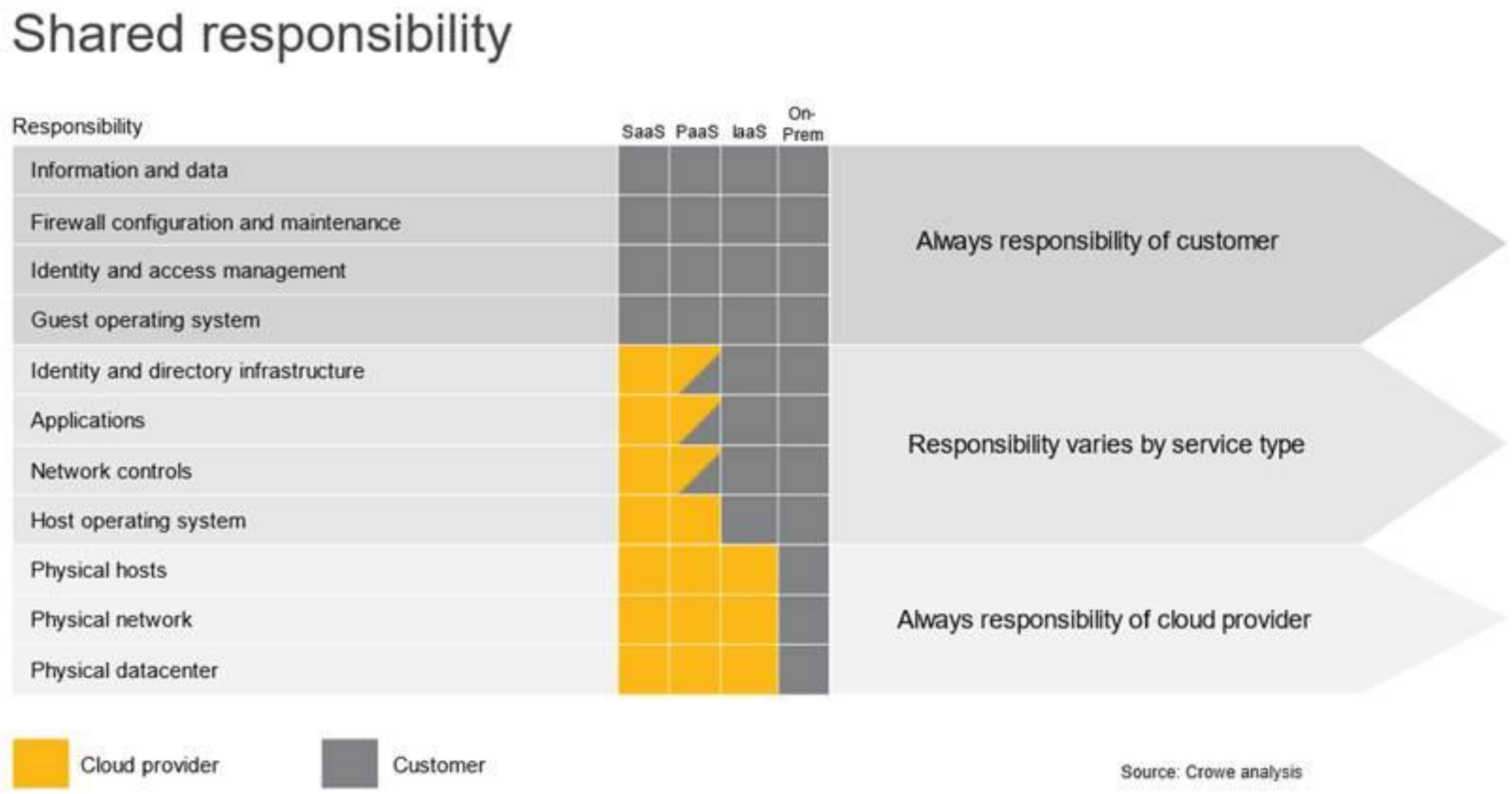


Application as a Service

Platform as a Service

Infrastructure as a Service

Cloud is still a Shared Responsibility



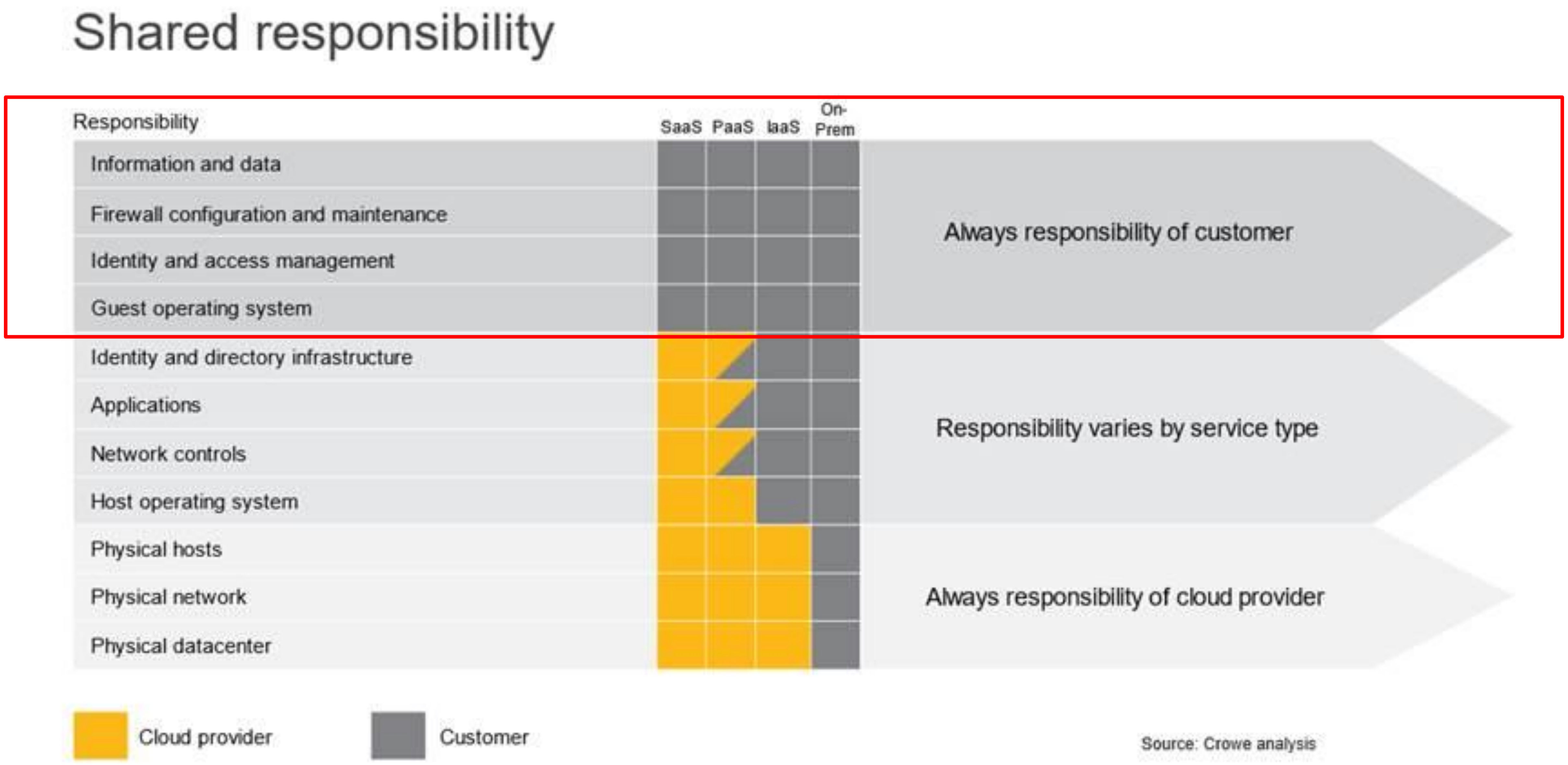
Shared responsibility

Responsibility	SaaS	PaaS	IaaS	On-Prem	
Information and data	⬛	⬛	⬛	⬛	Always responsibility of customer
Firewall configuration and maintenance	⬛	⬛	⬛	⬛	
Identity and access management	⬛	⬛	⬛	⬛	
Guest operating system	⬛	⬛	⬛	⬛	
Identity and directory infrastructure	🟨	🟨/⬛	⬛	⬛	Responsibility varies by service type
Applications	🟨	🟨/⬛	⬛	⬛	
Network controls	🟨	🟨/⬛	⬛	⬛	
Host operating system	🟨	🟨	⬛	⬛	
Physical hosts	🟨	🟨	🟨	⬛	Always responsibility of cloud provider
Physical network	🟨	🟨	🟨	⬛	
Physical datacenter	🟨	🟨	🟨	⬛	

🟨 Cloud provider ⬛ Customer

Source: Crowe analysis

Cloud is still a Shared Responsibility



Shared responsibility

Responsibility	SaaS	PaaS	IaaS	On-Prem	
Information and data	⬛	⬛	⬛	⬛	Always responsibility of customer
Firewall configuration and maintenance	⬛	⬛	⬛	⬛	
Identity and access management	⬛	⬛	⬛	⬛	
Guest operating system	⬛	⬛	⬛	⬛	
Identity and directory infrastructure	🟨	🟨/⬛	⬛	⬛	Responsibility varies by service type
Applications	🟨	🟨/⬛	⬛	⬛	
Network controls	🟨	🟨/⬛	⬛	⬛	
Host operating system	🟨	🟨	⬛	⬛	
Physical hosts	🟨	🟨	🟨	⬛	Always responsibility of cloud provider
Physical network	🟨	🟨	🟨	⬛	
Physical datacenter	🟨	🟨	🟨	⬛	

🟨 Cloud provider ⬛ Customer

Source: Crowe analysis

The Journey

	Phase I: Pre-Adoption	Phase II: Early Adoption	Phase III: Adoption	Phase IV: Mature
Current State	• A few third-party applications that are cloud-based • No cloud infrastructure • No major cloud applications like O365	• A few third-party applications that are cloud-based • No cloud infrastructure • At least one major cloud project underway or completed (O365)	• Multiple third-party applications that are cloud-based • Early stages or planned cloud infrastructure • At least one major cloud project completed (O365)	• Numerous third-party applications that are cloud-based • Implemented architecture for at least 1 - 3 years • Developing platform/applications in cloud
Philosophy	• Unsure on cloud future. • No plans for infrastructure in next 6 - 12 months.	• Early stage strategy for additional cloud migration • Possible plans for infrastructure in next 6 - 12 months.	• Strategy for additional cloud migration • Plans for infrastructure in next 6 - 12 months.	• Cloud is an ongoing component of IT strategy
Digital Transformation	• No or early stage strategy	• No or early stage strategy	• Robust strategy	• Robust strategy
Mindset	• May not see the value • Someone in the organization is opposed • Fearful of losing control • Little to no cloud expertise	• Being led by a third party app • May have a champion or two with specific needs provided by cloud • Some cloud expertise	• Have experienced demonstrated benefit • Looking to expand to gain additional value • May have acquired cloud expertise • Using major provider, likely partnering with 3rd party	• Seasoned cloud experience, understands value • Cloud is now standard • Most likely in house cloud expertise • Looking to optimize or take it to the next level

The Journey

	Phase I: Pre-Adoption	Phase II: Early Adoption	Phase III: Adoption	Phase IV: Mature
Areas of Focus	**Cloud Strategy** • Digital Transformation Strategy • Cloud Transformation Strategy • Governance • Migration Strategy **Cloud Management** • Third Party Mgmt. **Cloud Security** • Regulatory and Privacy Compliance • Cloud Access Security • Security Assessment **Cloud Transformation** • N/A	**Cloud Strategy** • Digital Transformation Strategy • Cloud Transformation Strategy • Governance • Migration Strategy **Cloud Management** • Third Party Mgmt. • Utilization and Financial Management • Cloud MDR **Cloud Security** • Regulatory and Privacy Compliance • Cloud Access Security • Security Configuration • Data Protection **Cloud Transformation** • Data Transformation • Technical Conversion **Software Development** • DevOps Transformation • Security DevOps	**Cloud Strategy** • Governance • Migration Strategy **Cloud Management** • Third Party Mgmt. • Utilization and Financial Management • Cloud MDR **Cloud Security** • Regulatory and Privacy Compliance • Cloud Access Security • Security Configuration • Data Protection • Offensive Cloud Testing **Cloud Transformation** • Data Transformation • Technical Conversion **Software Development** • DevOps Transformation • Security DevOps	**Cloud Strategy** • Governance **Cloud Management** • Third Party Mgmt. • Cloud MDR **Cloud Optimization** • Utilization and Financial Management **Cloud Security** • Regulatory and Privacy Compliance • Cloud Access Security • Security Configuration • Data Protection • Offensive Cloud Testing **Software Development** • DevOps Transformation • Security DevOps

The Process

One Time (Or Limited Times)

Step 1 - Define Digital Transformation Strategy

Step 2 - Define Cloud Strategy

Step 3 - Design Cloud Transformation Roadmap

Iterative

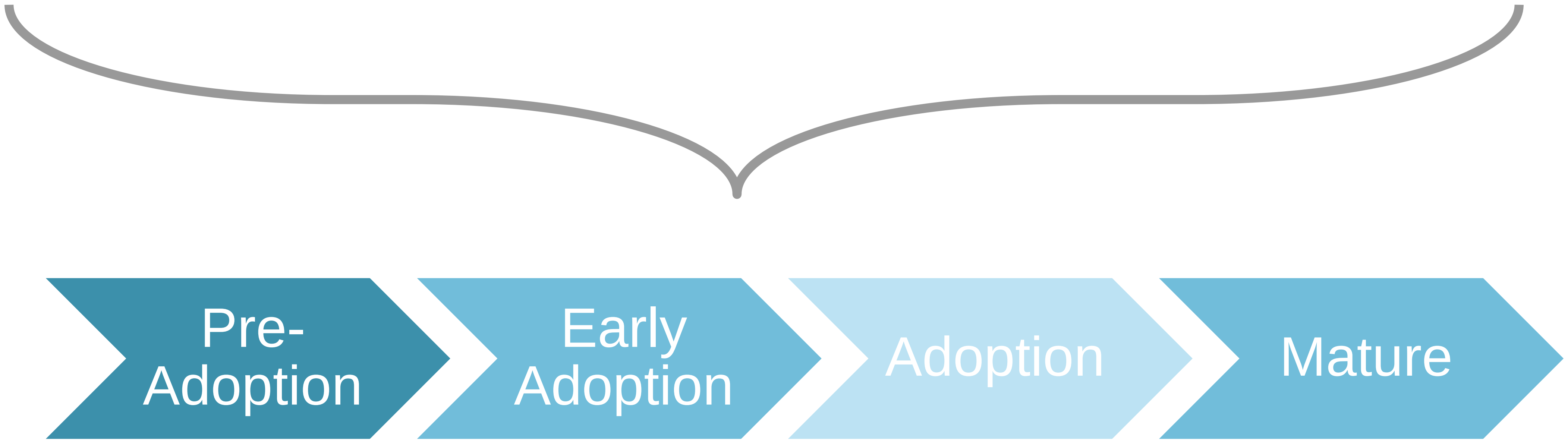
Step 4 - Define Governance, Security, Technical Design

Step 5 - Acquire Cloud Assets

Step 6 - Migrate, Test, Prod

Ongoing

Step 7 - Ongoing Optimization and Security Testing



Pre-Adoption → Early Adoption → Adoption → Mature

Developing your Cloud Strategy

Utilize your existing business strategy

Consider why/how Cloud will contribute to your strategy.

Design a thoughtful path forward

© 2020 Crowe LLP

The Top Three Challenges

1

Cost Management

- Licensing
- Resource Utilization
- Architecture

The Top Three Challenges

1

Cost Management

- Licensing
- Resource Utilization
- Architecture

2

Access Management

- Multi-Factor Authentication
- Guest Access Management
- Self–Service Management

The Top Three Challenges

1

Cost Management

- Licensing
- Resource Utilization
- Architecture

2

Access Management

- Multi-Factor Authentication
- Guest Access Management
- Self–Service Management

3

Resource Management

- Virtual Machine Disk Encryption
- Storage Encryption

Zero Trust

Zero Trust is a **security concept** where organizations **should not automatically trust** anything **inside** or **outside** its networks. Instead, **all connections** must be **verified before granting access**.

Zero Trust

Zero Trust is a **security concept** where organizations **should not automatically trust** anything **inside** or **outside** its networks. Instead, **all connections** must be **verified before granting access**.

Identity + Defined Resource Access + Continuous Trust Evaluation + Access Control

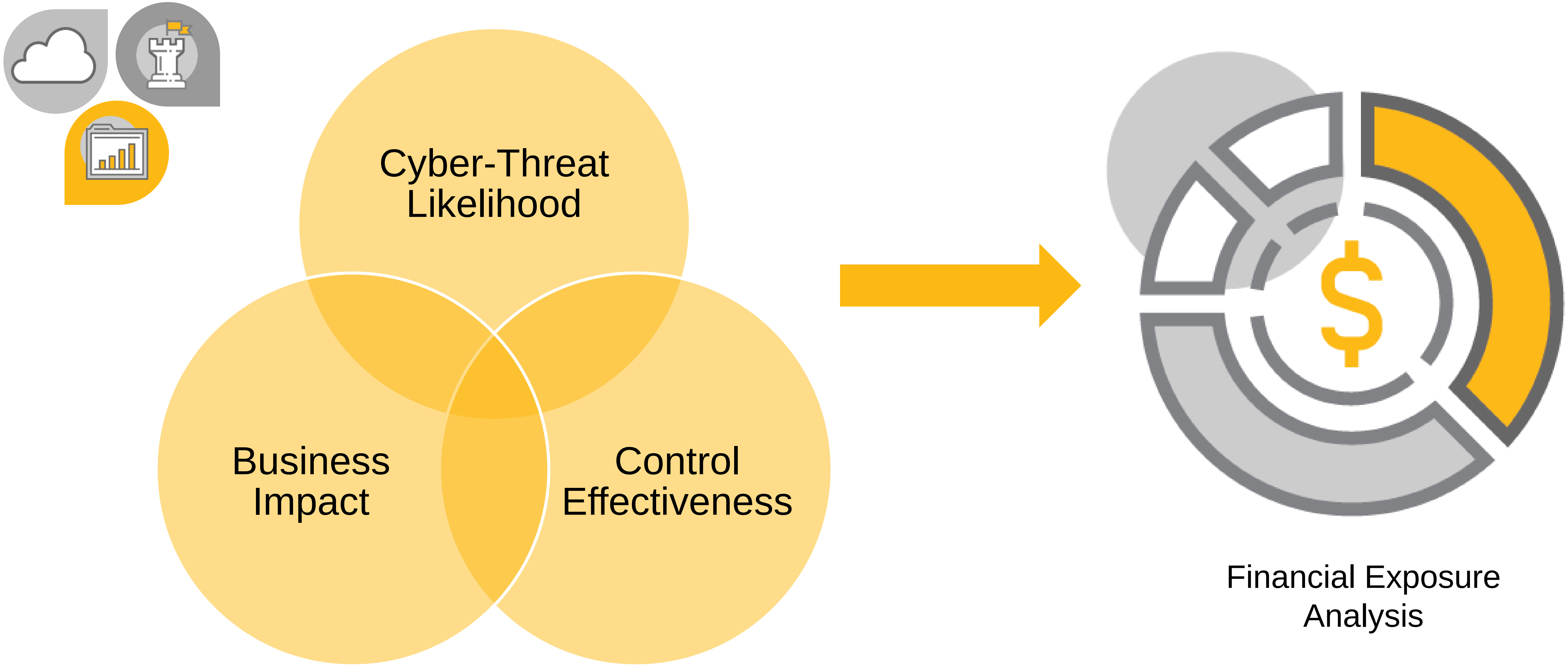
Getting Started…

Confirm what technologies and tools you have and are already using.

Similar to Cloud, develop a strategy

Leverage what you are building (new) as a change agent towards your strategy

Risk Quantification and Measurement



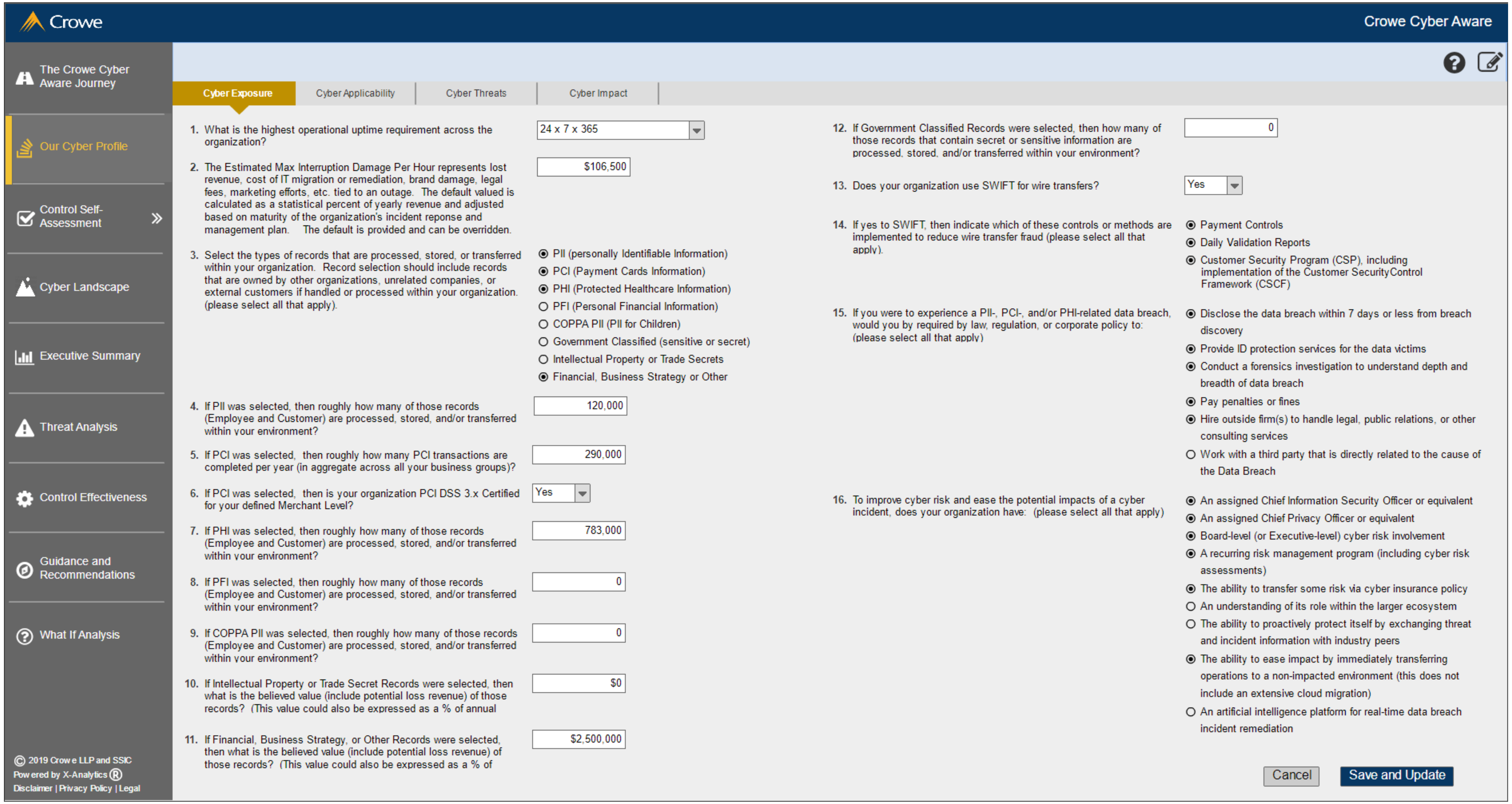
Cyber-Threat Likelihood

Business Impact

Control Effectiveness

Financial Exposure Analysis

Identifying Cyber Exposure



1. What is the highest operational uptime requirement across the organization? 24 x 7 x 365

2. The Estimated Max Interruption Damage Per Hour represents lost revenue, cost of IT migration or remediation, brand damage, legal fees, marketing efforts, etc. tied to an outage. The default valued is calculated as a statistical percent of yearly revenue and adjusted based on maturity of the organization's incident reponse and management plan. The default is provided and can be overridden. $106,500

3. Select the types of records that are processed, stored, or transferred within your organization. Record selection should include records that are owned by other organizations, unrelated companies, or external customers if handled or processed within your organization. (please select all that apply).
   - ● PII (personally Identifiable Information)
   - ● PCI (Payment Cards Information)
   - ● PHI (Protected Healthcare Information)
   - ○ PFI (Personal Financial Information)
   - ○ COPPA PII (PII for Children)
   - ○ Government Classified (sensitive or secret)
   - ○ Intellectual Property or Trade Secrets
   - ● Financial, Business Strategy or Other

4. If PII was selected, then roughly how many of those records (Employee and Customer) are processed, stored, and/or transferred within your environment? 120,000

5. If PCI was selected, then roughly how many PCI transactions are completed per year (in aggregate across all your business groups)? 290,000

6. If PCI was selected, then is your organization PCI DSS 3.x Certified for your defined Merchant Level? Yes

7. If PHI was selected, then roughly how many of those records (Employee and Customer) are processed, stored, and/or transferred within your environment? 783,000

8. If PFI was selected, then roughly how many of those records (Employee and Customer) are processed, stored, and/or transferred within your environment? 0

9. If COPPA PII was selected, then roughly how many of those records (Employee and Customer) are processed, stored, and/or transferred within your environment? 0

10. If Intellectual Property or Trade Secret Records were selected, then what is the believed value (include potential loss revenue) of those records? (This value could also be expressed as a % of annual $0

11. If Financial, Business Strategy, or Other Records were selected, then what is the believed value (include potential loss revenue) of those records? (This value could also be expressed as a % of $2,500,000

12. If Government Classified Records were selected, then how many of those records that contain secret or sensitive information are processed, stored, and/or transferred within your environment? 0

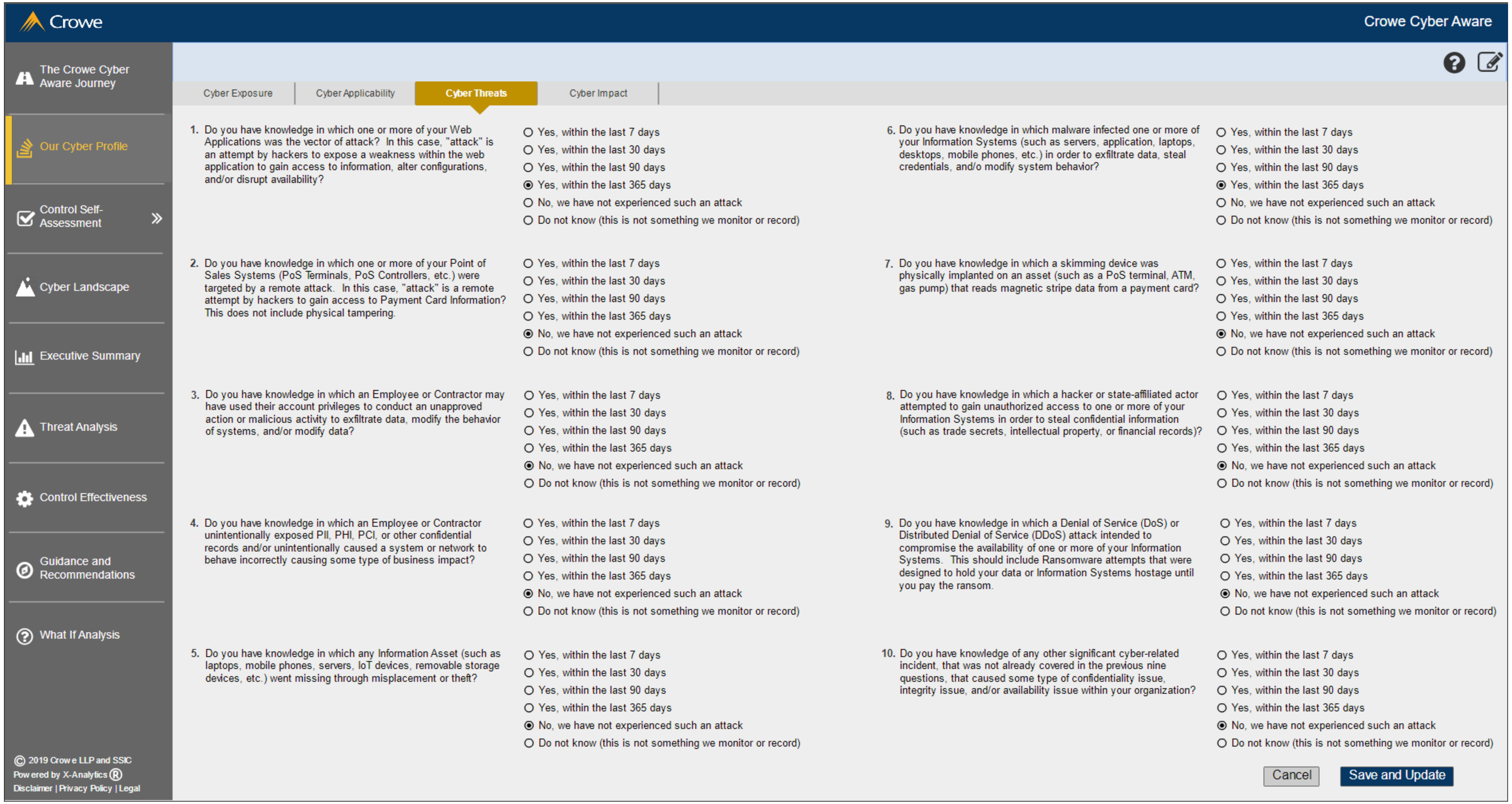
13. Does your organization use SWIFT for wire transfers? Yes

14. If yes to SWIFT, then indicate which of these controls or methods are implemented to reduce wire transfer fraud (please select all that apply).
    - ● Payment Controls
    - ● Daily Validation Reports
    - ● Customer Security Program (CSP), including implementation of the Customer SecurityControl Framework (CSCF)

15. If you were to experience a PII-, PCI-, and/or PHI-related data breach, would you by required by law, regulation, or corporate policy to: (please select all that apply)
    - ● Disclose the data breach within 7 days or less from breach discovery
    - ● Provide ID protection services for the data victims
    - ● Conduct a forensics investigation to understand depth and breadth of data breach
    - ● Pay penalties or fines
    - ● Hire outside firm(s) to handle legal, public relations, or other consulting services
    - ○ Work with a third party that is directly related to the cause of the Data Breach

16. To improve cyber risk and ease the potential impacts of a cyber incident, does your organization have: (please select all that apply)
    - ● An assigned Chief Information Security Officer or equivalent
    - ● An assigned Chief Privacy Officer or equivalent
    - ● Board-level (or Executive-level) cyber risk involvement
    - ● A recurring risk management program (including cyber risk assessments)
    - ● The ability to transfer some risk via cyber insurance policy
    - ○ An understanding of its role within the larger ecosystem
    - ○ The ability to proactively protect itself by exchanging threat and incident information with industry peers
    - ● The ability to ease impact by immediately transferring operations to a non-impacted environment (this does not include an extensive cloud migration)
    - ○ An artificial intelligence platform for real-time data breach incident remediation

Identifying Cyber Threats



1. Do you have knowledge in which one or more of your Web Applications was the vector of attack? In this case, "attack" is an attempt by hackers to expose a weakness within the web application to gain access to information, alter configurations, and/or disrupt availability?
   - ○ Yes, within the last 7 days
   - ○ Yes, within the last 30 days
   - ○ Yes, within the last 90 days
   - ● Yes, within the last 365 days
   - ○ No, we have not experienced such an attack
   - ○ Do not know (this is not something we monitor or record)

2. Do you have knowledge in which one or more of your Point of Sales Systems (PoS Terminals, PoS Controllers, etc.) were targeted by a remote attack. In this case, "attack" is a remote attempt by hackers to gain access to Payment Card Information? This does not include physical tampering.
   - ○ Yes, within the last 7 days
   - ○ Yes, within the last 30 days
   - ○ Yes, within the last 90 days
   - ○ Yes, within the last 365 days
   - ● No, we have not experienced such an attack
   - ○ Do not know (this is not something we monitor or record)

3. Do you have knowledge in which an Employee or Contractor may have used their account privileges to conduct an unapproved action or malicious activity to exfiltrate data, modify the behavior of systems, and/or modify data?
   - ○ Yes, within the last 7 days
   - ○ Yes, within the last 30 days
   - ○ Yes, within the last 90 days
   - ○ Yes, within the last 365 days
   - ● No, we have not experienced such an attack
   - ○ Do not know (this is not something we monitor or record)

4. Do you have knowledge in which an Employee or Contractor unintentionally exposed PII, PHI, PCI, or other confidential records and/or unintentionally caused a system or network to behave incorrectly causing some type of business impact?
   - ○ Yes, within the last 7 days
   - ○ Yes, within the last 30 days
   - ○ Yes, within the last 90 days
   - ○ Yes, within the last 365 days
   - ● No, we have not experienced such an attack
   - ○ Do not know (this is not something we monitor or record)

5. Do you have knowledge in which any Information Asset (such as laptops, mobile phones, servers, IoT devices, removable storage devices, etc.) went missing through misplacement or theft?
   - ○ Yes, within the last 7 days
   - ○ Yes, within the last 30 days
   - ○ Yes, within the last 90 days
   - ○ Yes, within the last 365 days
   - ● No, we have not experienced such an attack
   - ○ Do not know (this is not something we monitor or record)

6. Do you have knowledge in which malware infected one or more of your Information Systems (such as servers, application, laptops, desktops, mobile phones, etc.) in order to exfiltrate data, steal credentials, and/o modify system behavior?
   - ○ Yes, within the last 7 days
   - ○ Yes, within the last 30 days
   - ○ Yes, within the last 90 days
   - ● Yes, within the last 365 days
   - ○ No, we have not experienced such an attack
   - ○ Do not know (this is not something we monitor or record)

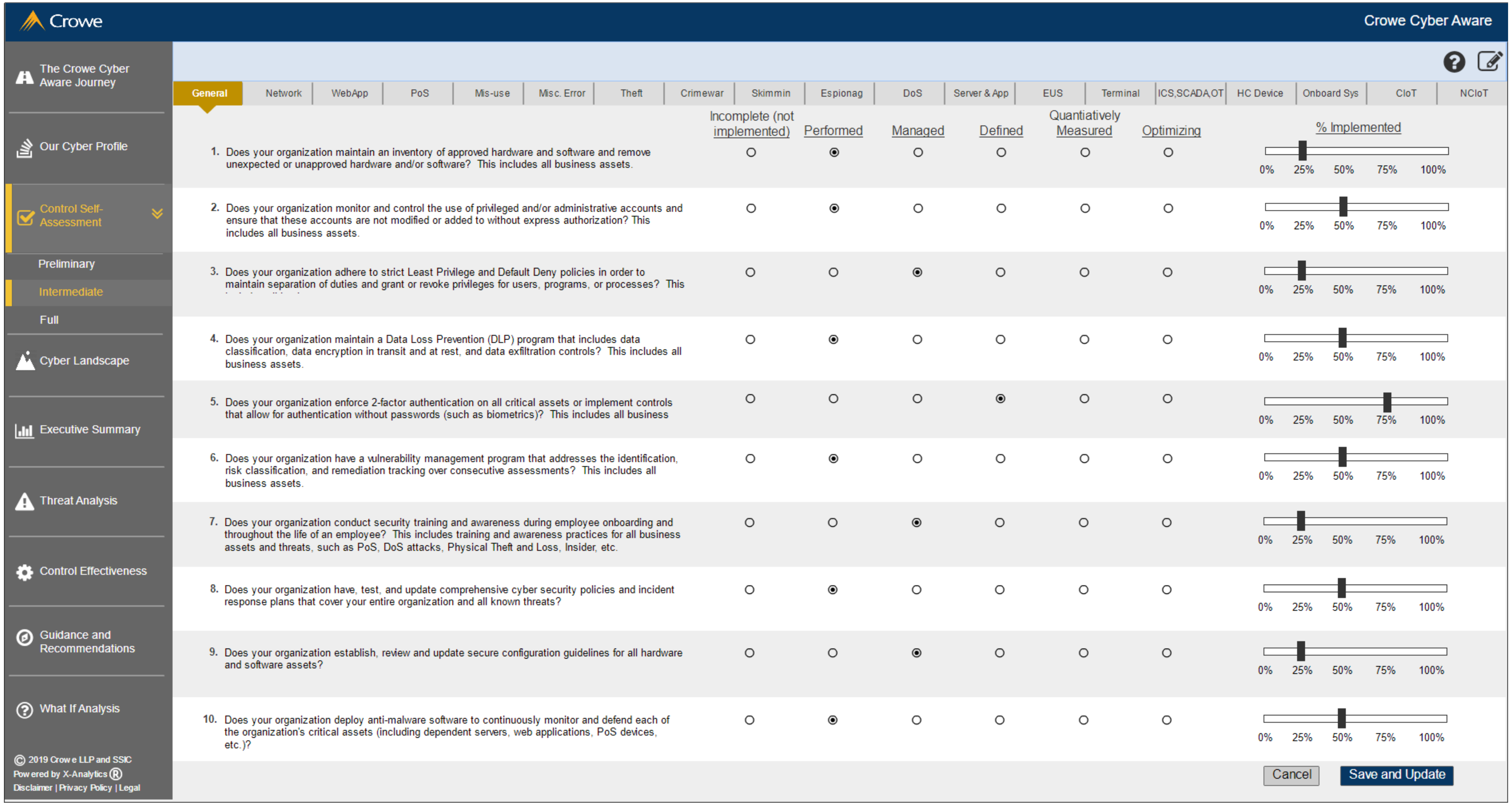
7. Do you have knowledge in which a skimming device was physically implanted on an asset (such as a PoS terminal, ATM, gas pump) that reads magnetic stripe data from a payment card?
   - ○ Yes, within the last 7 days
   - ○ Yes, within the last 30 days
   - ○ Yes, within the last 90 days
   - ○ Yes, within the last 365 days
   - ● No, we have not experienced such an attack
   - ○ Do not know (this is not something we monitor or record)

8. Do you have knowledge in which a hacker or state-affiliated actor attempted to gain unauthorized access to one or more of your Information Systems in order to steal confidential information (such as trade secrets, intellectual property, or financial records)?
   - ○ Yes, within the last 7 days
   - ○ Yes, within the last 30 days
   - ○ Yes, within the last 90 days
   - ○ Yes, within the last 365 days
   - ● No, we have not experienced such an attack
   - ○ Do not know (this is not something we monitor or record)

9. Do you have knowledge in which a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack intended to compromise the availability of one or more of your Information Systems. This should include Ransomware attempts that were designed to hold your data or Information Systems hostage until you pay the ransom.
   - ○ Yes, within the last 7 days
   - ○ Yes, within the last 30 days
   - ○ Yes, within the last 90 days
   - ○ Yes, within the last 365 days
   - ● No, we have not experienced such an attack
   - ○ Do not know (this is not something we monitor or record)

10. Do you have knowledge of any other significant cyber-related incident, that was not already covered in the previous nine questions, that caused some type of confidentiality issue, integrity issue, and/or availability issue within your organization?
    - ○ Yes, within the last 7 days
    - ○ Yes, within the last 30 days
    - ○ Yes, within the last 90 days
    - ○ Yes, within the last 365 days
    - ● No, we have not experienced such an attack
    - ○ Do not know (this is not something we monitor or record)

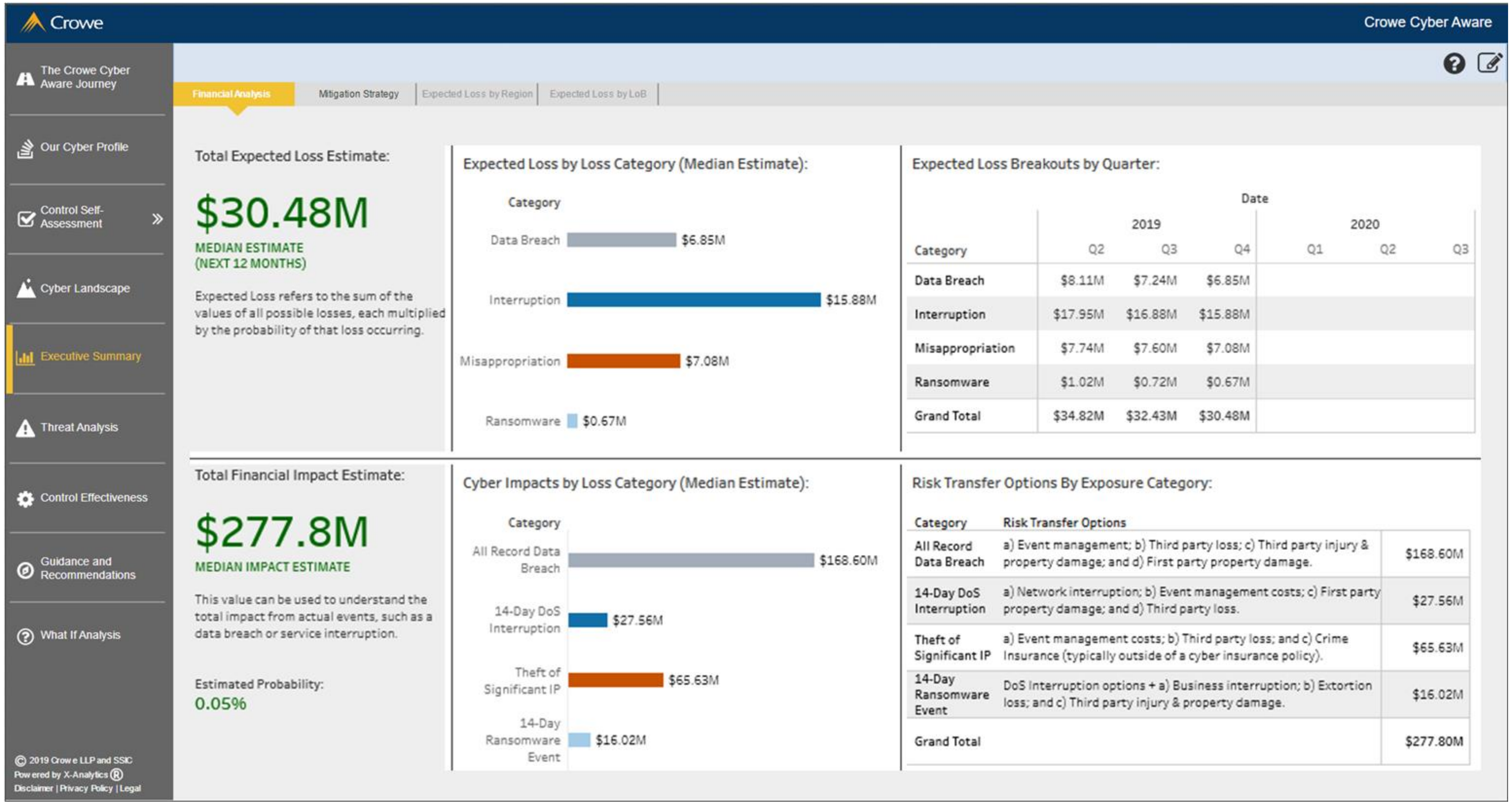
Aiding in Control Self-Assessment



	Incomplete (not implemented)	Performed	Managed	Defined	Quantitatively Measured	Optimizing	% Implemented
1. Does your organization maintain an inventory of approved hardware and software and remove unexpected or unapproved hardware and/or software? This includes all business assets.	○	●	○	○	○	○	0% [✓ 25%] 50% 75% 100%
2. Does your organization monitor and control the use of privileged and/or administrative accounts and ensure that these accounts are not modified or added to without express authorization? This includes all business assets.	○	●	○	○	○	○	0% 25% [✓ 50%] 75% 100%
3. Does your organization adhere to strict Least Privilege and Default Deny policies in order to maintain separation of duties and grant or revoke privileges for users, programs, or processes? This	○	○	●	○	○	○	0% [✓ 25%] 50% 75% 100%
4. Does your organization maintain a Data Loss Prevention (DLP) program that includes data classification, data encryption in transit and at rest, and data exfiltration controls? This includes all business assets.	○	●	○	○	○	○	0% 25% [✓ 50%] 75% 100%
5. Does your organization enforce 2-factor authentication on all critical assets or implement controls that allow for authentication without passwords (such as biometrics)? This includes all business	○	○	○	●	○	○	0% 25% 50% [✓ 75%] 100%
6. Does your organization have a vulnerability management program that addresses the identification, risk classification, and remediation tracking over consecutive assessments? This includes all business assets.	○	●	○	○	○	○	0% 25% [✓ 50%] 75% 100%
7. Does your organization conduct security training and awareness during employee onboarding and throughout the life of an employee? This includes training and awareness practices for all business assets and threats, such as PoS, DoS attacks, Physical Theft and Loss, Insider, etc.	○	○	●	○	○	○	0% [✓ 25%] 50% 75% 100%
8. Does your organization have, test, and update comprehensive cyber security policies and incident response plans that cover your entire organization and all known threats?	○	●	○	○	○	○	0% 25% [✓ 50%] 75% 100%
9. Does your organization establish, review and update secure configuration guidelines for all hardware and software assets?	○	○	●	○	○	○	0% [✓ 25%] 50% 75% 100%
10. Does your organization deploy anti-malware software to continuously monitor and defend each of the organization's critical assets (including dependent servers, web applications, PoS devices, etc.)?	○	●	○	○	○	○	0% 25% [✓ 50%] 75% 100%

© 2019 Crowe LLP and SSIC
Powered by X-Analytics ®
Disclaimer | Privacy Policy | Legal

Executive Summary – Financial Analysis



© 2019 Crowe LLP and SSIC
Powered by X-Analytics®
Disclaimer | Privacy Policy | Legal

Total Expected Loss Estimate:

$30.48M

MEDIAN ESTIMATE
(NEXT 12 MONTHS)

Expected Loss refers to the sum of the values of all possible losses, each multiplied by the probability of that loss occurring.

Expected Loss by Loss Category (Median Estimate):

Expected Loss Breakouts by Quarter:

	Date					
	2019			2020		
Category	Q2	Q3	Q4	Q1	Q2	Q3
Data Breach	$8.11M	$7.24M	$6.85M			
Interruption	$17.95M	$16.88M	$15.88M			
Misappropriation	$7.74M	$7.60M	$7.08M			
Ransomware	$1.02M	$0.72M	$0.67M			
Grand Total	$34.82M	$32.43M	$30.48M			

Total Financial Impact Estimate:

$277.8M

MEDIAN IMPACT ESTIMATE

This value can be used to understand the total impact from actual events, such as a data breach or service interruption.

Estimated Probability:
0.05%

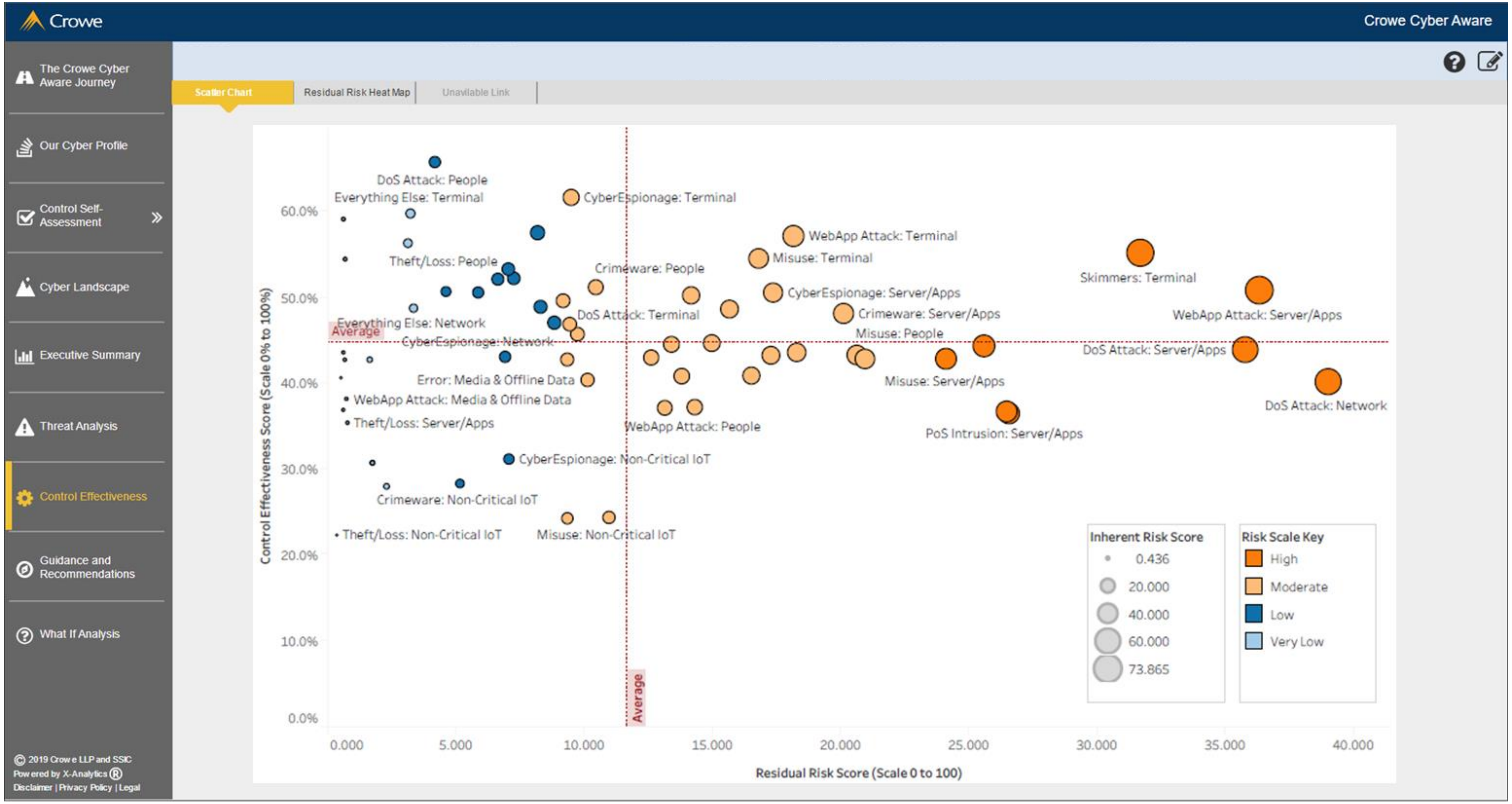
Cyber Impacts by Loss Category (Median Estimate):

Category
All Record Data Breach $168.60M
14-Day DoS Interruption $27.56M
Theft of Significant IP $65.63M
14-Day Ransomware Event $16.02M

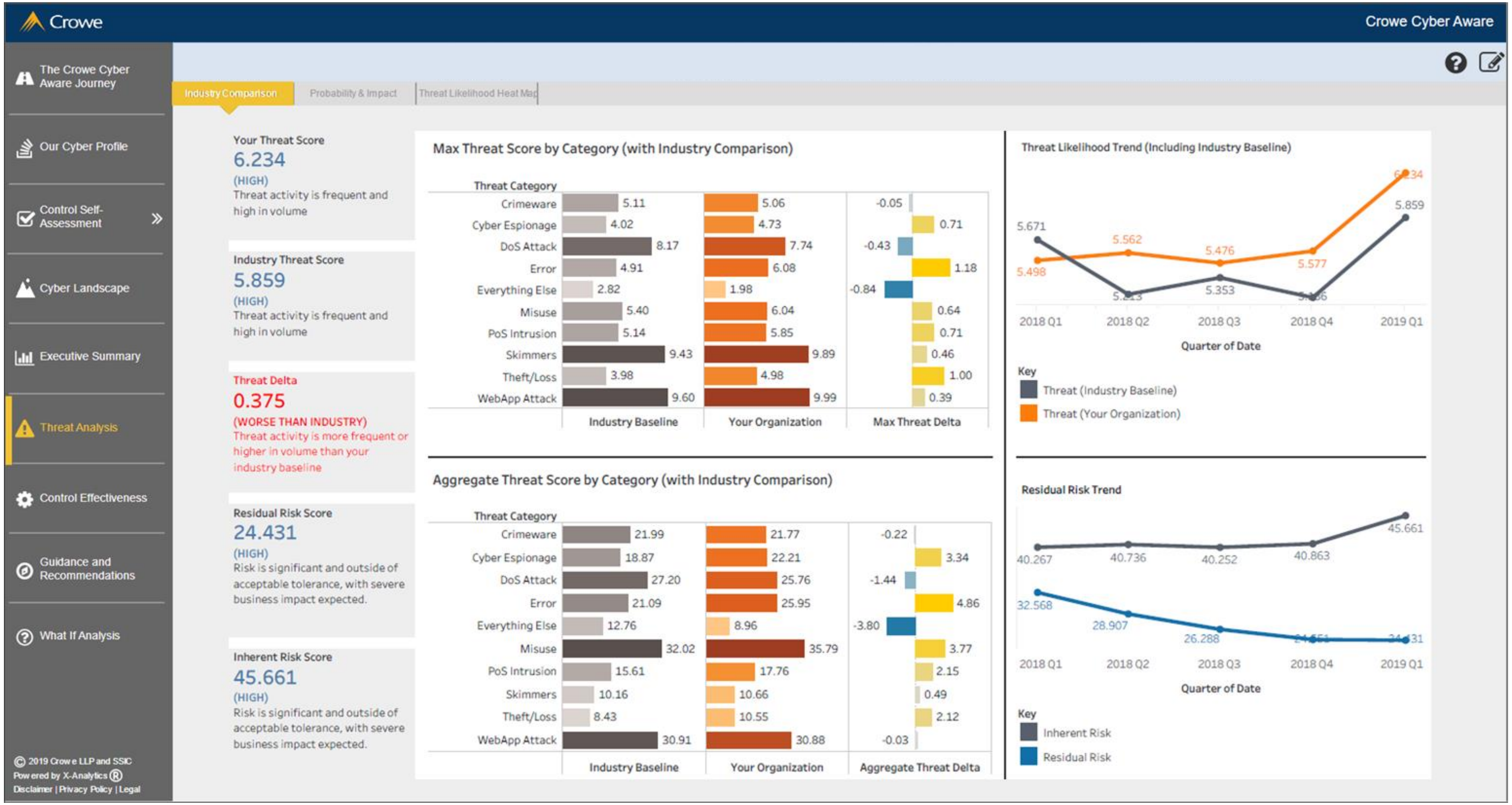
Risk Transfer Options By Exposure Category:

Category	Risk Transfer Options	
All Record Data Breach	a) Event management; b) Third party loss; c) Third party injury & property damage; and d) First party property damage.	$168.60M
14-Day DoS Interruption	a) Network interruption; b) Event management costs; c) First party property damage; and d) Third party loss.	$27.56M
Theft of Significant IP	a) Event management costs; b) Third party loss; and c) Crime Insurance (typically outside of a cyber insurance policy).	$65.63M
14-Day Ransomware Event	DoS Interruption options + a) Business interruption; b) Extortion loss; and c) Third party injury & property damage.	$16.02M
Grand Total		$277.80M

Control Effectiveness – Display Example



Control Effectiveness – Display Example


Crowe
Crowe Cyber Aware
The Crowe Cyber Aware Journey
Our Cyber Profile
Control Self-Assessment
Cyber Landscape
Executive Summary
Threat Analysis
Control Effectiveness
Guidance and Recommendations
What If Analysis
© 2019 Crowe LLP and SSC
Powered by X-Analytics®
Disclaimer | Privacy Policy | Legal
Industry Comparison
Probability & Impact
Threat Likelihood Heat Map
Max Threat Score by Category (with Industry Comparison)
Threat Category
Crimeware 5.11 5.06 -0.05
Cyber Espionage 4.02 4.73 0.71
DoS Attack 8.17 7.74 -0.43
Error 4.91 6.08 1.18
Everything Else 2.82 1.98 -0.84
Misuse 5.40 6.04 0.64
PoS Intrusion 5.14 5.85 0.71
Skimmers 9.43 9.89 0.46
Theft/Loss 3.98 4.98 1.00
WebApp Attack 9.60 9.99 0.39
Industry Baseline
Your Organization
Max Threat Delta
Aggregate Threat Score by Category (with Industry Comparison)
Threat Category
Crimeware 21.99 21.77 -0.22
Cyber Espionage 18.87 22.21 3.34
DoS Attack 27.20 25.76 -1.44
Error 21.09 25.95 4.86
Everything Else 12.76 8.96 -3.80
Misuse 32.02 35.79 3.77
PoS Intrusion 15.61 17.76 2.15
Skimmers 10.16 10.66 0.49
Theft/Loss 8.43 10.55 2.12
WebApp Attack 30.91 30.88 -0.03
Industry Baseline
Your Organization
Aggregate Threat Delta
Threat Likelihood Trend (Including Industry Baseline)
5.671
5.498
5.562
5.476
5.353
5.577
6.234
5.859
2018 Q1
2018 Q2
2018 Q3
2018 Q4
2019 Q1
Quarter of Date
Key
Threat (Industry Baseline)
Threat (Your Organization)
Residual Risk Trend
40.267
40.736
40.252
40.863
45.661
32.568
28.907
26.288
24.431
2018 Q1
2018 Q2
2018 Q3
2018 Q4
2019 Q1
Quarter of Date
Key
Inherent Risk
Residual Risk

Your Threat Score
6.234
(HIGH)
Threat activity is frequent and high in volume

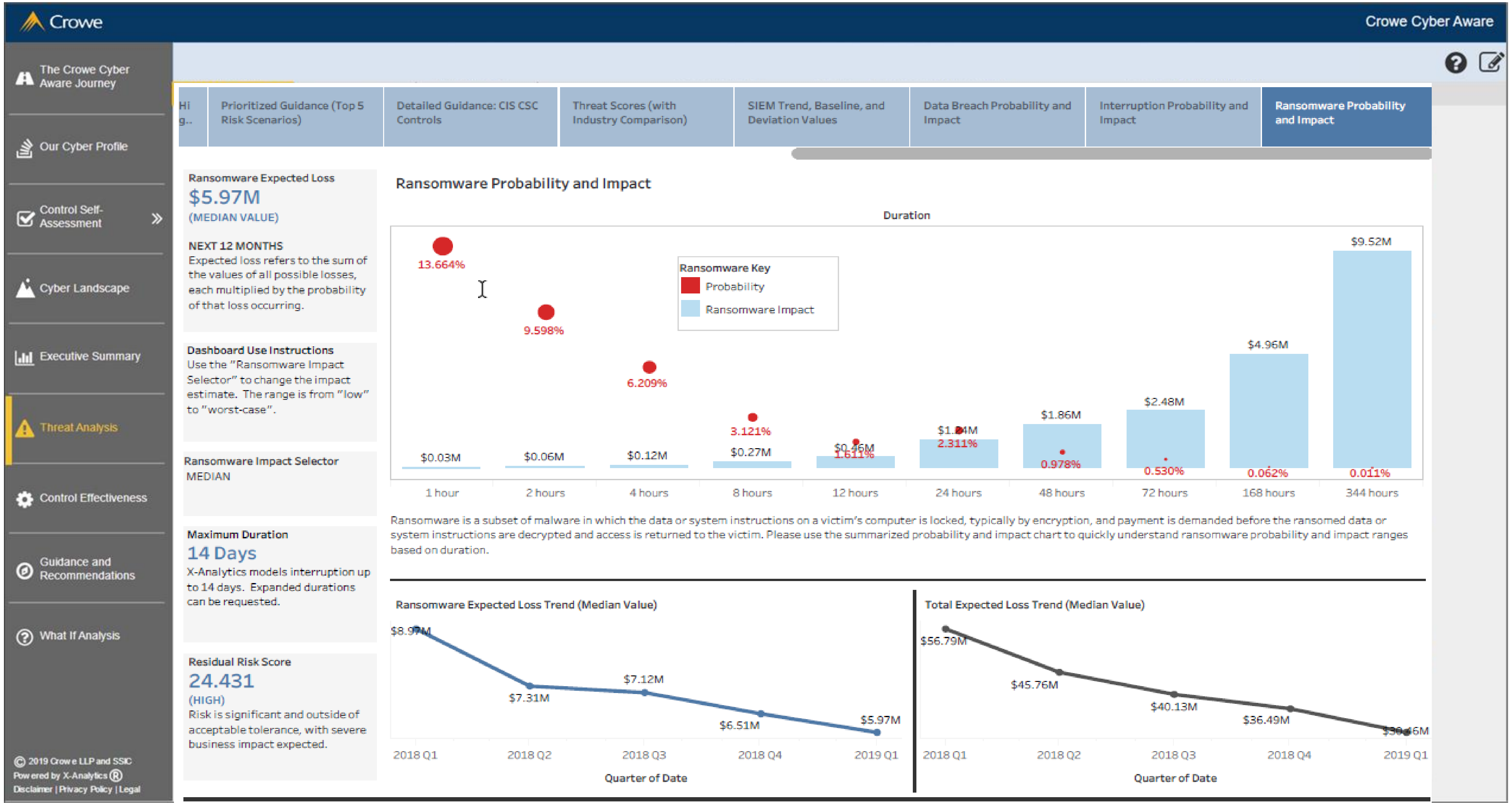
Industry Threat Score
5.859
(HIGH)
Threat activity is frequent and high in volume

Threat Delta
0.375
(WORSE THAN INDUSTRY)
Threat activity is more frequent or higher in volume than your industry baseline

Residual Risk Score
24.431
(HIGH)
Risk is significant and outside of acceptable tolerance, with severe business impact expected.

Inherent Risk Score
45.661
(HIGH)
Risk is significant and outside of acceptable tolerance, with severe business impact expected.

Ransomware Probability and Impact



Ransomware Expected Loss
$5.97M
(MEDIAN VALUE)

NEXT 12 MONTHS
Expected loss refers to the sum of the values of all possible losses, each multiplied by the probability of that loss occurring.

Dashboard Use Instructions
Use the "Ransomware Impact Selector" to change the impact estimate. The range is from "low" to "worst-case".

Ransomware Impact Selector
MEDIAN

Maximum Duration
14 Days
X-Analytics models interruption up to 14 days. Expanded durations can be requested.

Residual Risk Score
24.431
(HIGH)
Risk is significant and outside of acceptable tolerance, with severe business impact expected.

Ransomware Probability and Impact

Ransomware is a subset of malware in which the data or system instructions on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data or system instructions are decrypted and access is returned to the victim. Please use the summarized probability and impact chart to quickly understand ransomware probability and impact ranges based on duration.

Ransomware Expected Loss Trend (Median Value)

Total Expected Loss Trend (Median Value)

Building Information Security Momentum

Utilize Known Frameworks

Rely on creditable and referenceable cybersecurity guidance and direction.

Understand Your Risks

Establish a Cybersecurity Risk Appetite Statement and Tolerance.

Invest Where It Counts

Consider how your IT investments will better Operations, Customers, and your Business Strategy.

Always consider your Cyber Risk Tolerance.

Communicate Roles and Apply Accountability

Ramp up frequency and depth of communication related to cybersecurity (board, committees, sub-committees)

Accountability. Separation of Duties.

Validate how your organizations Cyber/IT areas are structured

Whom is owning what, how are responsibilities aligned, what skillsets are necessary.

Confirm.

Consider the appropriate forums to ensure actions, investments, and risks are united.

Ask all questions; if you cannot ask the question, find someone whom can.

Measure.

Reconsider what you are measuring; and how often.

Keep your Risk Appetite at the forefront.

Crowe

Thank You

“Crowe” is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. Crowe may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global. The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

Dave McKnight, CISSP
Principal, Crowe Consulting
dave.mcknight@crowe.com
630.575.4399

Dave works with mid-sized financial services organizations to refine their cybersecurity capabilities. He is a Principal at Crowe LLP and co-leads Crowe's Digital Security for Financial Services practice.

He began his professional career by testing the security thresholds of corporate networks and deployed applications, fulfilling various InfoSec roles for his clients along the way. Over sixteen years, Dave has assisted directors, executives, and boards with prioritizing and assessing their cybersecurity goals and risk posture. By providing increased organizational awareness, cybersecurity maturity discussion, and executing real-world attack simulations, Dave is dedicated to helping organizations up their cybersecurity game, no matter where they are right now.