Cybersecurity Risk in Private Equity

Actions to Manage Cost & Risk to Address Cybersecurity

June 2021

Housekeeping

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. If your question is not addressed in the session, a Crowe professional will follow up with you.
- 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
- Participate for at least 50 minutes
- Successfully complete 3 of the 4 polling questions

NO CPE CREDIT

- Failure to successfully complete 3 of the 4 polling questions
- Viewing a recording of this session (CPE is only awarded for live sessions)

CPE CERTIFICATE OF COMPLETION

Will be available for download following the session and e-mailed within two weeks of successfully passing this program

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

Cybersecurity Risk in Private Equity

Actions to Manage Cost & Risk to Address Cybersecurity

June 2021

Today’s Agenda

- Introductions
- Cybersecurity Risks
- Cybersecurity Assessments
- Security Awareness Training
- Incident Detection and Response
- Questions

Chris Wilkinson
Principal
+1 219 308 8980
christopher.wilkinson@crowe.com

Michael Salihoglu
Manager
+1 312 759 1027
michael.salihoglu@crowe.com

Polling Question #1

<u>Password policy for company X:</u>
Length: 8 characters
Complexity required: Three of the four (A, a, 1, !)
Lockout: 3 Attempts
Lockout duration: Forever

QUESTION: Given the above password complexity is enabled on the system, what would be ***your first guess*** for user account passwords?

A) June2021

B) Cowboys2021

C) Password1

D) Crowe123

Cybersecurity Risks

Cybersecurity Capabilities

- How vulnerable is the company to Cyber attacks?
- How do I ensure the proper controls are in place around Cybersecurity?
- Are employees properly trained on how to protect the company against Cybersecurity threats?
- Has Cybersecurity governance been established in portfolio companies?

- Can you be sure the company hasn't already been hacked?
- Does the company have the ability to detect suspicious activity and/or successful breach attempts?

- Has the organization fully met data privacy laws/regulations (HIPAA, PCI, GDPR, CCPA, etc.)?
- Has the company implemented a Disaster Recovery plan including sufficient data backups?

- Does the organization have the capabilities and skills to respond to a Cybersecurity breach?
- Do IT personnel understand what to do in the event of a breach?

Cybersecurity Control Framework

CYBERSECURITY GOVERNANCE

POLICIES AND PROCEDURES
- Information Security Program
- Standard Operating Procedures
- Administrative Standards

ROLES AND RESPONSIBILITIES
- Organizational Structure
- Information Security Officer
- Security Responsibilities

OVERSIGHT AND STRATEGY

IT RISK MANAGEMENT
- IT Risk Definition
- Risk Appetite / Tolerance
- Risk and Control Universe
- Risk Assessment
- Risk Treatment
- Communication Plan
- Risk Monitoring

CYBERSECURITY DOMAINS

DATA PROTECTION
- Data Classification
- Data Inventory
- Data Protection Controls Framework
- Encryption
- Data Destruction

THREAT AND VULNERABILITY MANAGEMENT
- Anti-Virus Standards
- Vulnerability Management Programs
- Patch Management
- Incident Response

PHYSICAL SECURITY
- Documentation Storage and Security
- Clean Desk Policy
- Data Center Physical Security

LOGICAL SECURITY
- Authentication
- Access Management (User Requests and Terminations)
- User Access Reviews
- Segregation of Duties

LOGGING AND MONITORING
- Application / Database
- Server
- Network / Wireless
- Log Aggregation
- SIEM

IT OPERATIONS
- IT Asset Management
- Scheduled Job Security

BUSINESS CONTINUITY MANAGEMENT
- Business Impact Assessment
- Contingency Plans
- Critical IT Systems Redundancy
- Disaster Planning
- Backup Processes

THIRD-PARTY RISK MANAGEMENT
- Data Sharing Inventory
- Security Review – Vendor Selection
- Security Review – Ongoing
- Third-Party Network Access
- Contracts

EMPLOYEE MANAGEMENT
- Hiring Practices
- Security Training
- Employee Policies and Standards

SECURITY CONFIGURATION MANAGEMENT
- Approved Infrastructure
- Standard Build Procedures
- Configuration Certification

SECURITY CHANGE MANAGEMENT
- Change Management
- System Integration

SECURE DEVELOPMENT
- Secure Design
- Secure Coding Practices
- Secure Development
- Security Testing

IT COMPLIANCE
- FFIEC Cybersecurity Assessment Tool
- HIPAA Security and Privacy
- PCI
- NAIC Model Audit Rule

The Cost of Ransomware

According to Sophos, the average cost of remediating a ransomware attack more than doubled in the past year, ***from $761,106 in 2020 to $1.85M in 2021.****

* "The State of Ransomware 2021," Sophos, April 27, 2021, https://www.sophos.com/en-us/press-office/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year.aspx

Ransomware in 2021

Key Takeaways:

- Dramatic increase in success in 2020 into 2021, why?
- How do these attacks happen?
- Who is being targeted?
- Attacks have become more sophisticated. How?

Ransomware [preparedness]

Tactically, what should we be reviewing?

- ✓**Email content filtering:** What is able to be delivered to employees?
- ✓**Security awareness:** How well are employees trained?
- ✓**Endpoint protection:** Is there a layered approach?
- ✓**Propagation:** Are we limiting the avenues for privilege escalation, including local administrator? Share permissions?
- ✓**Data backups:** Have procedures been tested?
- ✓**Data exfiltration:** What channels of communication are available outbound?
- ✓**Incident response**: Can we respond in a timely manner with the right skills?

Polling Question #2

QUESTION: Where would you rate your company/companies with regard to addressing Cybersecurity risk?

A) Just beginning to address Cybersecurity risk

B) An assessment has been performed and a roadmap exists

C) Significant progress has been made based on assessment results

D) The organization has a mature Cybersecurity program in place

Cybersecurity Assessments

Phase One: Cyber-Risk Profiling

- ✓ Cyber-Risk profile built for each portfolio company based on **customized survey** of 10-20 questions/criteria (sample below)
- ✓ Overall **risk score calculated** and companies are tiered based on survey results
- ✓ **Cyber assessment prescription** and schedule built for each tier of companies
- ✓ Survey can be incorporated into **due diligence** work for potential Cyber risk of future companies

Portfolio Company	Industry	Cyber-Risk Rating
PORTCO1	Retail	*87*
PORTCO2	Healthcare	*65*
PORTCO3	Education	*41*

Please enter the name of your organization.	✓ Industry	What sensitive information do you store, transmit, or process?	How many third parties do you share sensitive information with?	Is your IT function in-house, or outsourced?	How many employees do you have?	How many IT employees and/or IT contractors do you have?	How many people are dedicated to the information security function?	How many security incidents have you experienced in the last two years?
PORTCO1	Retail	Customer Credit Card Information (PCI), Employee Health Records (HIPAA), Trade secrets, other internally sensitive information	11-20	In-house	1,001-5,000	<10	No formal security function exists	1-2
PORTCO2	Healthcare	Health Records (HIPAA), Social Security numbers, date and place of birth, Trade secrets	1-10	Outsourced except CIO	501-1,000	51-150	Outsourced security function	3-5

Phase Two: Cyber Assessments Identify Your Exposure

PREVENT

Option A: Cybersecurity Health Check

Best for situations where:

- Companies are just getting started addressing Cybersecurity
- Policies and procedures may or may not exist
- Limited testing with tools to get high-level data on areas of improvement
- Organization wants to determine the maturity of Cybersecurity controls at a high level
- Remote capabilities to perform assessment

Approach:

- Policy and procedure review to ensure governance
- Limited use of Cyber toolset to test settings
- High-level interview with key IT resources to review processes

Option B: Cybersecurity Assessment "In-Depth Assessment"

Best for situations where:

- Organizations have established at least an initial Cybersecurity program
- Policies and procedures have not been reviewed
- Cyber toolset used to identify vulnerabilities in systems
- Analysis of Cyber maturity to provide strategic and tactical roadmap

Approach:

- Policy and procedure review to ensure governance
- Use of Cyber toolset to test settings
- Interview with key IT resources to review processes
- Follow-up testing in 6-9 months to track progress

Option C: Penetration Testing "Ethical Hacking"

Best for situations where:

- Organizations have previously performed a Cybersecurity assessment and addressed gaps
- Company is comfortable with current Cyber policies and procedures
- Intense real-world hacking exercise of all systems is valuable to prevent attacks
- Optional Phishing and Wireless testing can be added to scope

Approach:

- Comprehensive Penetration Testing of all internal and external systems
- Follow-up testing in 6-9 months to track progress

Cybersecurity Assessments: Takeaways

Not all companies carry the same amount of risk!

- Perform an initial risk assessment to focus the efforts if resource or budget constraints are in place
- All companies (that have digital assets) do carry ***some*** risk
  - Sensitive data is a variable, not a constant

Assessment results: How to interpret the gaps?

- All companies should not be graded on the same test
- Tie vulnerabilities (gaps) back to top threats (Ransomware, malicious employee, etc.)
- Focus on the impact to the business – set flags for penetration testing
- Follow up in six months to ensure progress
- Many common gaps can be addressed at the PEG level
  - Policies and procedures, governance, toolsets, etc.

Polling Question #3

QUESTION: How mature is your security awareness training program?

A) We haven’t started on a training program

B) Informal training occurs but no tools are in place currently

C) A training program exists but employees are not tested

D) We have a formal training program that includes testing employees

Security Awareness Training

Spear Phishing Example

From: “Client Content Filter System" <client-web-filter@FAKEBUTLOOKSREAL.org>
Subject: Potential Acceptable Use Violation

Ryan,
Our web traffic monitoring service has reported that your account has visited potentially malicious web sites, including sites that are restricted per ABC’s Acceptable Use Policy.

We do realize that this type of activity is often caused by viruses and other types of malware. The following link will direct you to the detailed report of the malicious web sites your system has visited as reported by the monitoring service; please review this list for accuracy.

https://www.FAKEBUTLOOKSREAL.org/ABC/?sessionid=ryan.reynolds@abc.com

The file has been encrypted for privacy and requires Microsoft Word macros to be enabled for viewing. If you believe that any of the sites listed in the report have been reported erroneously or that all sites noted are false positives, please reply to this email and a manual review will be conducted by Information Security.

Employee Security Awareness: Takeaways

Raising the level of security awareness comes down to one thing…

CULTURE!!

1. Employees need to be tested: There are many tools available to perform testing in-house
   - Costs are reasonable and can be as low as $6/user/year if licenses are bundled

2. Employees need to be aware of the testing: This will ensure they are more diligent when real attacks happen

3. Reward those who do the right thing: Create a culture where those who report suspicious activity are recognized
   - Punishing those who fail is less effective
   - Recognition in a company newsletter only costs time!

4. Technical controls to mitigate the human element:
   - Email and web content filtering, advanced endpoint protection, and others…

Polling Question #4

QUESTION: How would you describe your ability to detect malicious activity on your systems?

A) Unknown

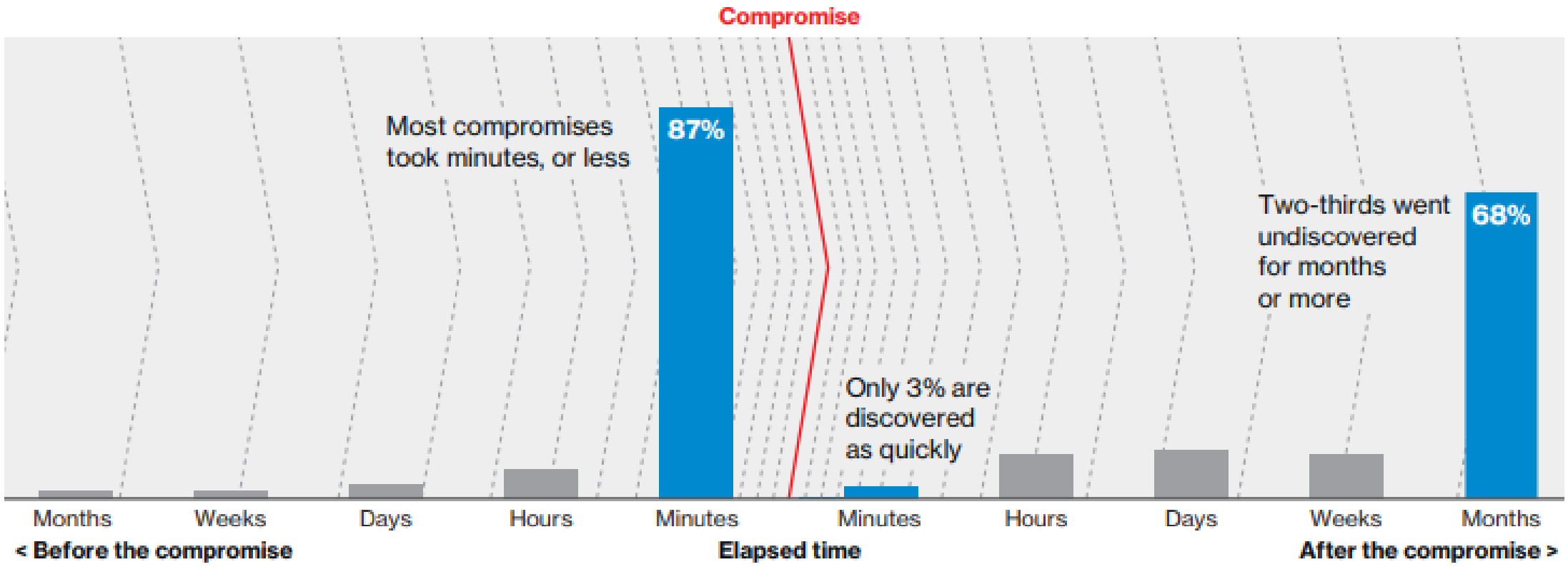
B) IT maintains system logs and monitors traffic internally

C) We have internal/outsourced capabilities that provide 24x7 monitoring

D) We have 24x7 capabilities and test effectiveness on a regular basis

Incident Detection and Response

Response Time



Source: 2018 Verizon Data Breach Investigations Report

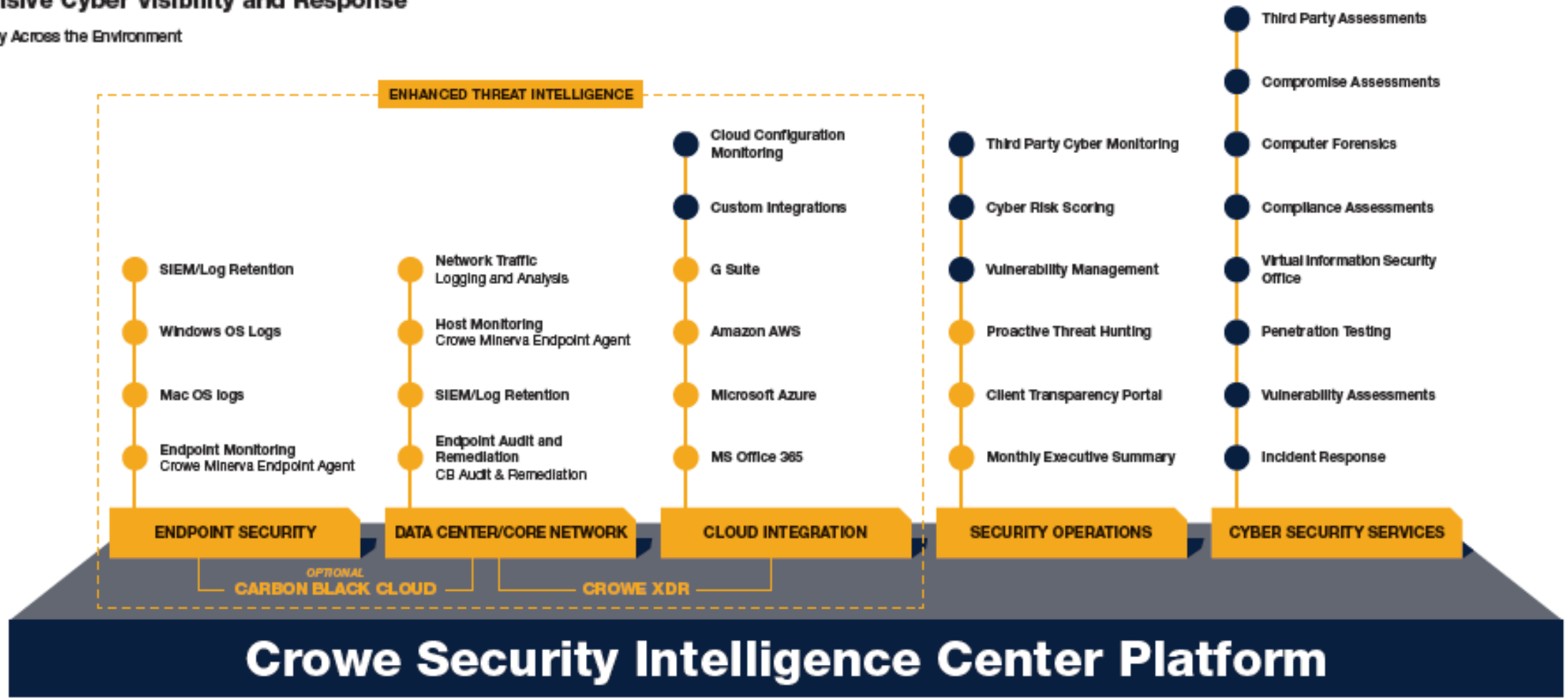
Prevention is Great, Detection is Critical…

DETECT

Security Intelligence Center

Comprehensive Cyber Visibility and Response

7x24x365 Visibility Across the Environment



Be Prepared – Incident Response Planning

27% of organizations don’t have a breach response plan or team in place*

37% have not reviewed or updated their plan since it was created*

- ✓What will I do?
- ✓What are the laws?
- ✓What will my regulator say?
- ✓How much will my customers ask?
- ✓Who will I call?
- ✓How do I stop it?
- ✓Have I tested my current plan?

* Based on Crowe client assessments

Thank You

Chris Wilkinson

+1 219 308 8980

christopher.wilkinson@crowe.com

Michael Salihoglu

+1 312 759 1027

michael.salihoglu@crowe.com