Crowe

Smart decisions. Lasting value.™

Private Equity: Assessing Cybersecurity Across the Portfolio

December 12, 2018

Today’s speakers

Chris Wilkinson, Principal
Crowe LLP
Christopher.wilkinson@crowe.com
Cell: 219.308.8980

Kiel Murray, Senior Manager
Crowe LLP
kiel.murray@crowe.com
Cell: 814.450.2800

John Kurkowski, Partner
Crowe LLP
john.kurkowski@crowe.com
Cell: 312.560.1257

Today’s discussion goals

- Welcome and introductions
- Think like an attacker!
- Cybersecurity primer
- Cybersecurity assessments
- Phase one: Portfolio company prioritization
- Phase two: Assessment of risk
- Questions and closing remarks

Think like an attacker!

Password policy for company X:

Length: 8 characters

Complexity required: Three of the four (A, a, 1, !)

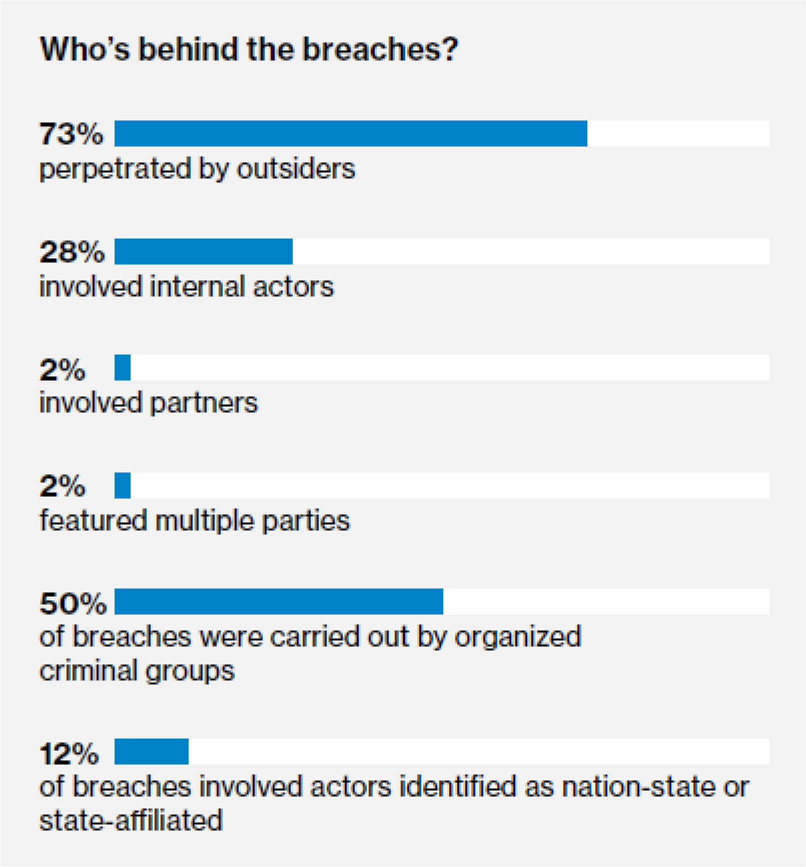
Lockout: 3 Attempts

Lockout duration: Forever

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

Cybersecurity primer

Threat actors



Who's behind the breaches?

73% perpetrated by outsiders

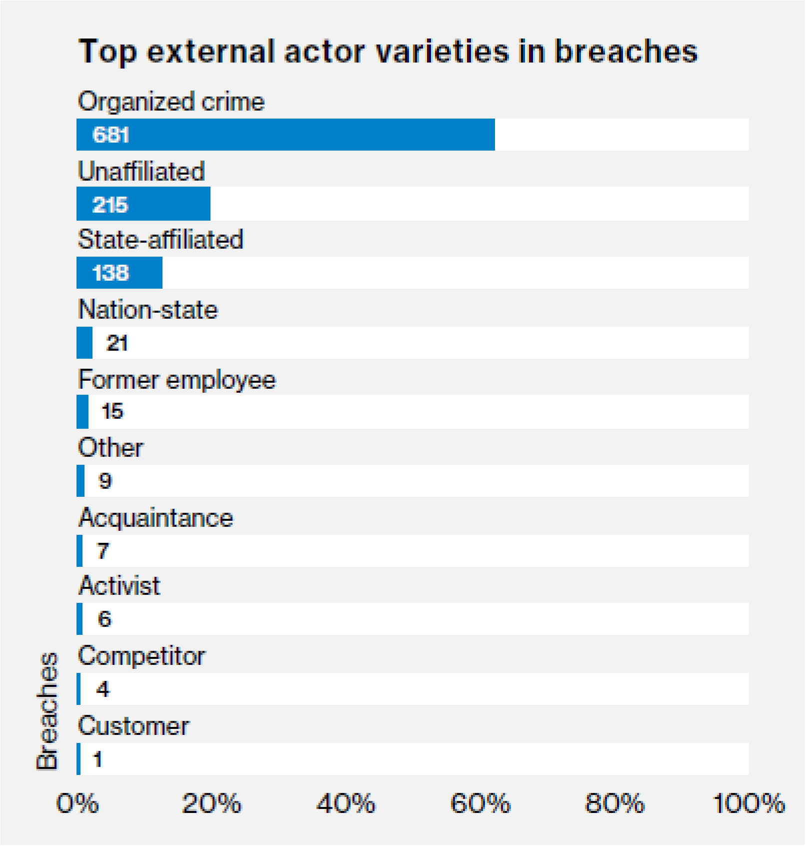
28% involved internal actors

2% involved partners

2% featured multiple parties

50% of breaches were carried out by organized criminal groups

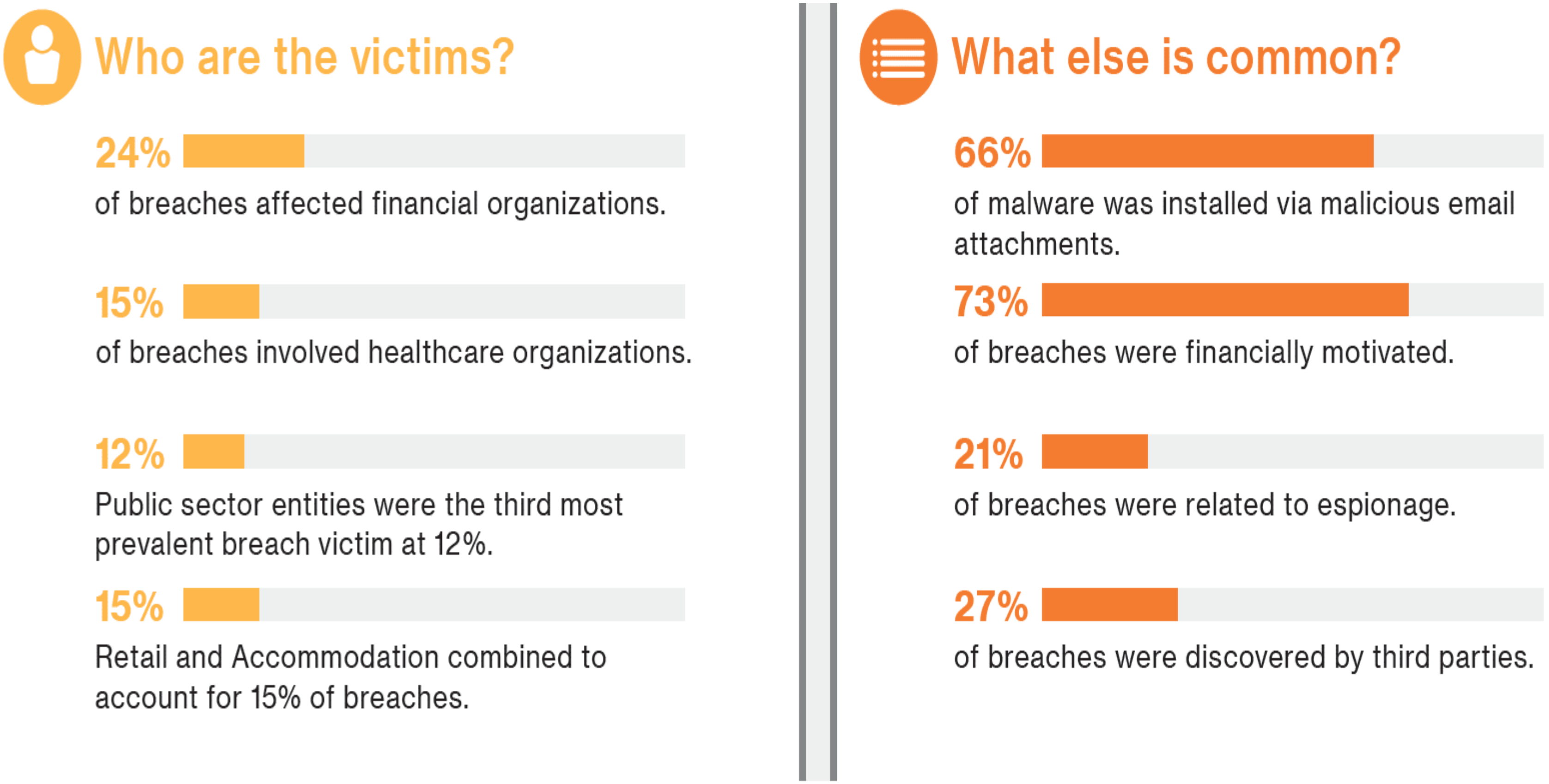
12% of breaches involved actors identified as nation-state or state-affiliated



Top external actor varieties in breaches

Source: 2018 Verizon Data Breach Investigations Report

Who is targeted?



Who are the victims?

24%

of breaches affected financial organizations.

15%

of breaches involved healthcare organizations.

12%

Public sector entities were the third most prevalent breach victim at 12%.

15%

Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66%

of malware was installed via malicious email attachments.

73%

of breaches were financially motivated.

21%

of breaches were related to espionage.

27%

of breaches were discovered by third parties.

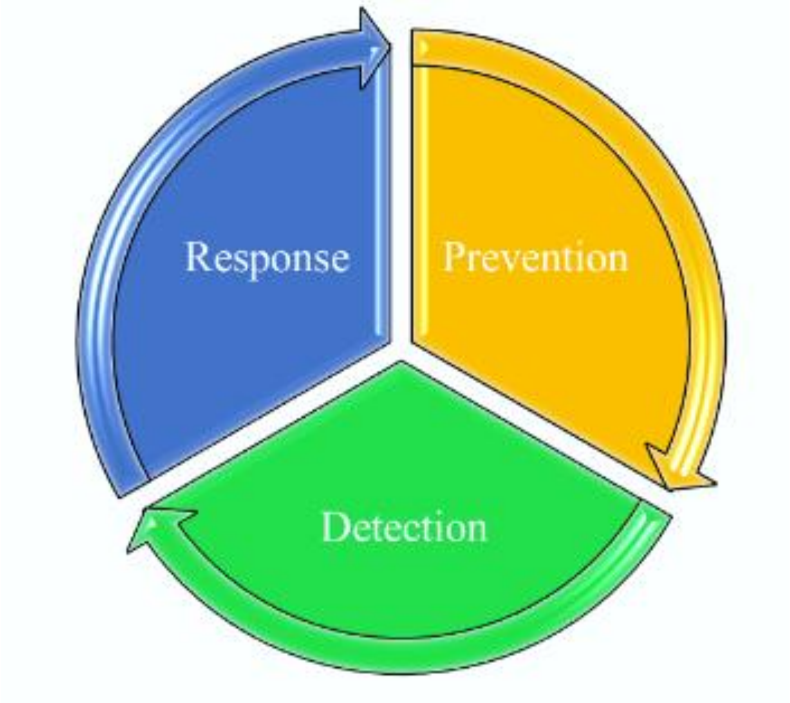
Prevention, detection, and response

It’s not a matter of ‘if’, it’s a matter of ‘when’

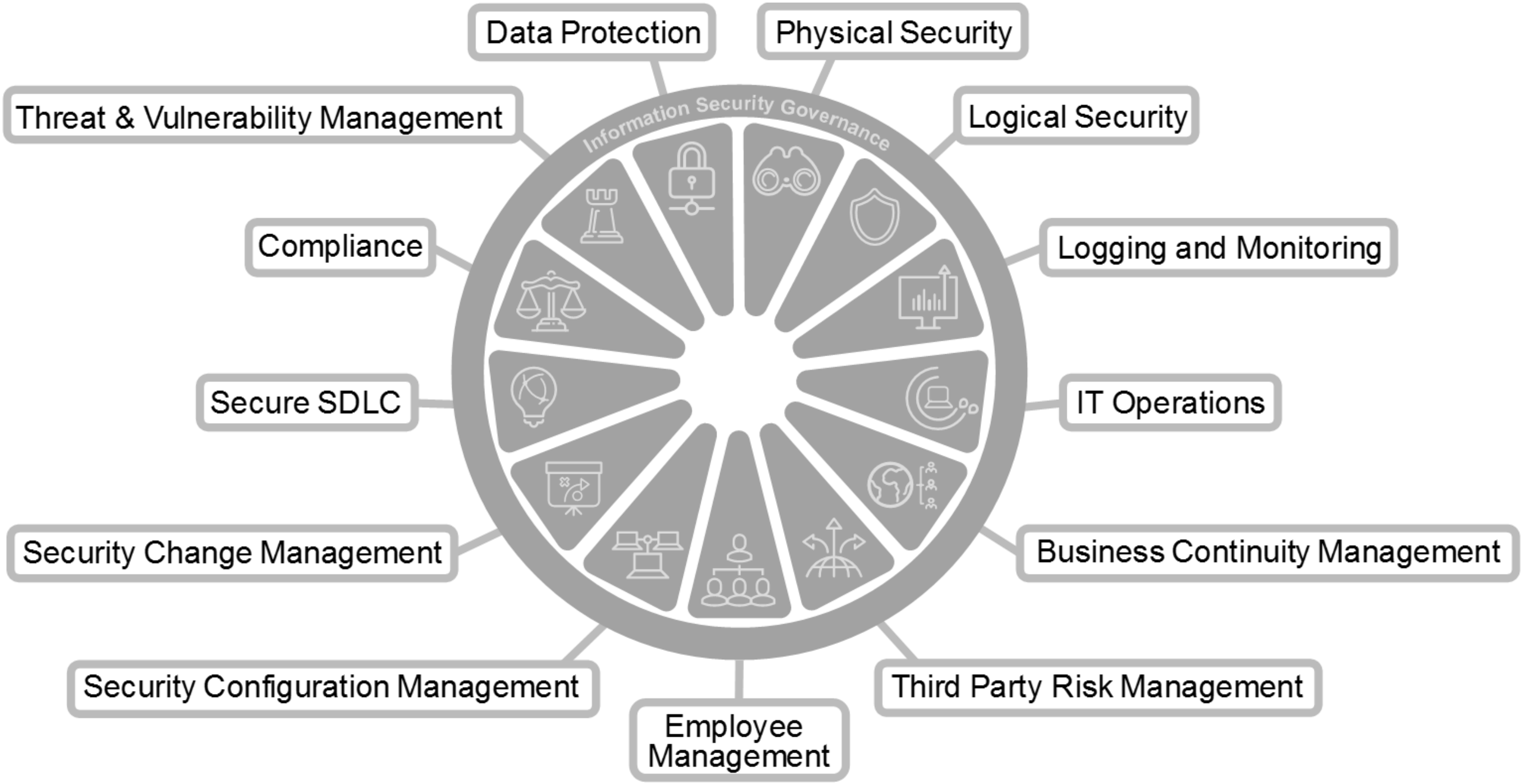
Three-phased strategy:

- Prevention
- Detection
- Response

To be able detect attacks that were not able to be prevented and to be able to limit damage by responding swiftly



Cybersecurity universe


Data Protection
Physical Security
Threat & Vulnerability Management
Information Security Governance
Logical Security
Compliance
Logging and Monitoring
Secure SDLC
IT Operations
Security Change Management
Business Continuity Management
Security Configuration Management
Third Party Risk Management
Employee Management

Cybersecurity risk and control framework

CYBERSECURITY GOVERNANCE

POLICIES AND PROCEDURES

- □ Information Security Program
- □ Standard Operating Procedures
- □ Administrative Standards

ROLES AND RESPONSIBILITIES

- □ Organizational Structure
- □ Security Responsibilities

OVERSIGHT AND STRATEGY

IT RISK MANAGEMENT

- □ IT Risk Definition
- □ Risk Appetite / Tolerance
- □ Risk Assessment
- □ Risk Monitoring

CYBERSECURITY DOMAINS

DATA PROTECTION

- □ Data Classification
- □ Data Inventory
- □ 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

- □ Security Training
- □ Employee Policies and Standards

SECURITY CONFIGURATION MANAGEMENT

- □ 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

Cybersecurity assessments

Phase one: Portfolio company prioritization

Risk factors to consider

- Industry and geography
- Types of data (PCI, HIPAA, IP, Employee, etc.)
- Volume of sensitive data
- Sharing of data with third parties/vendors
- IT and InfoSec team characteristics
- Incidents experienced
- Past assessments performed

Portfolio company – cyber-risk profiling

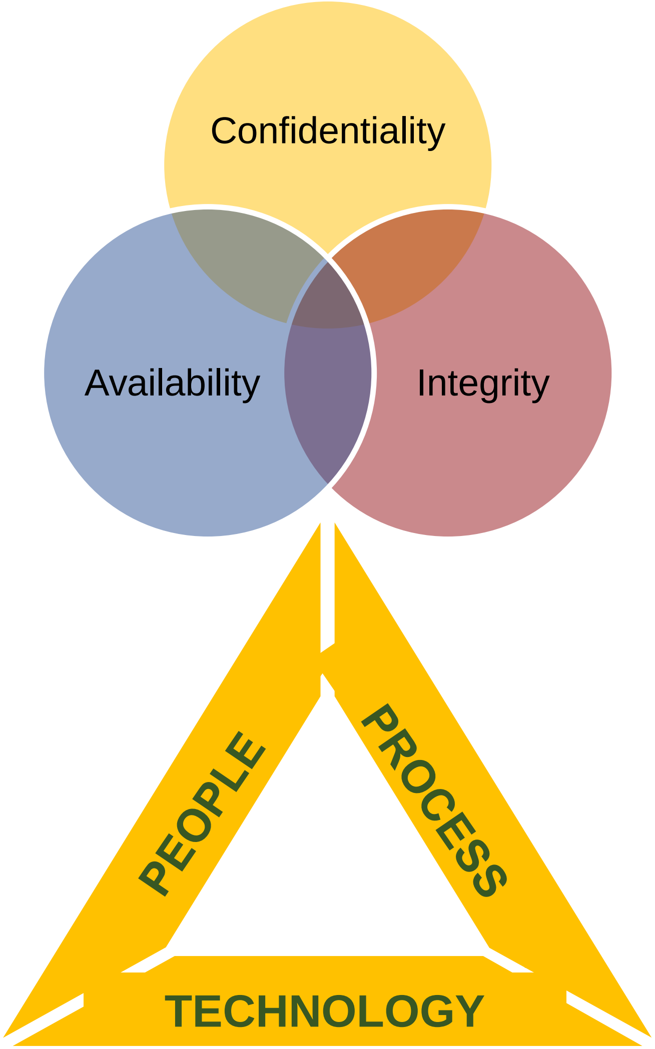
- ✓ Cyber-Risk profile built for each portfolio company based on **customized survey** of 10-20 questions/criteria (sample below)
- ✓ Overall **risk score calculated** and companies are tiered based on survey results
- ✓ **Cyber assessment prescription** and schedule built for each tier of companies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

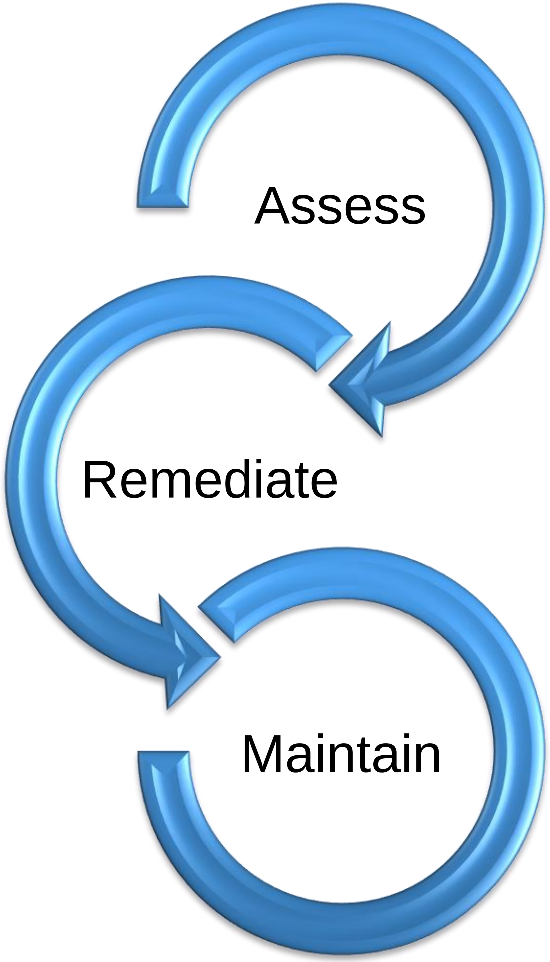
Portfolio Company	Industry	Cyber-Risk Rating
PORTCO1	Retail	*87*
PORTCO2	Healthcare	*65*
PORTCO3	Education	*41*

Company name	Industry	What sensitive information do you store, transmit, or process?	How many 3rd parties do you share data with?	IT function in-house?	How many employees do you have?	How many IT employees do you have?	People dedicated to information security?	Security incidents in the last two years?
PORTCO1	Retail	Customer Credit Card Information (PCI); Trade secrets, other internal information	11-20	Outsourced	1,001-5,000	<10	No formal security function exists	1-2
PORTCO2	Healthcare	Health Records (HIPAA);Social security numbers,	50-100	In-house	5K-10K	51-150	Outsourced security function	3-5

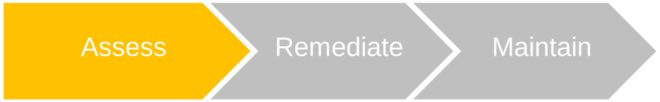
Phase two: Assessment of risk

Factors to consider





Cybersecurity health check


Assess

Remediate

Maintain

Best for situations where:

- Companies are just getting started addressing cybersecurity
- Policies and procedures have been developed but not reviewed
- Limited testing with tools to get high level data on areas of improvement
- Organization wants to determine the maturity of cybersecurity domains at a high level

Approach:

- Focus on governance: approximately 25 hours of effort
- Cybersecurity policy and procedures review
- Interview with key IT resources
- Limited tool scanning

Limitations:

- Review of control design only
- Limited insight to vulnerabilities

Penetration testing

Assess
Remediate
Maintain

Best for situations where:

- Organizations have previously performed a cybersecurity assessment and addressed gaps
- Company is comfortable with current cyber policies and procedures
- Real-world hacking exercise of all systems, answers “What could an attacker actually do?”
- Other areas such as phishing and wireless testing can be added to scope

Approach:

- Depending on scope of systems: 60-80 hours of effort is typical
- Comprehensive testing of all internal and Internet facing systems
- Determine organizations ability to detect, contain and respond to activity

Limitations:

- Review of control design is not performed, only operating effectiveness
- Policies and procedures typically not covered

Hybrid assessment

Assess

Remediate

Maintain

Best for situations where:

- Organizations have established at least an initial cybersecurity program
- Policies and procedures have not been reviewed
- Penetration testing has not been performed

Approach:

- Focus on strategic and tactical areas: approximately 40 hours of effort
- Limited penetration testing to provide insight to high risk areas
- Analysis of maturity across cybersecurity domains
- Review of policies and procedures
- Interviews with key IT resources

Limitations:

- Lack of comprehensive testing, focus on high risk areas
- Limited insight to vulnerabilities

Cybersecurity assessments – areas of coverage

Scope – area of coverage	Health check	Hybrid assessment	Penetration testing
Cyber-Risk Profile Assessment	Yes	Yes	Yes
Cyber-Threat Analysis	Yes	Yes	Yes
Sensitive Data Classification	Yes	Yes	Yes
Policies and Procedures Review	Yes	Yes	
Interview Key IT Resources	Yes	Yes	
Vulnerability Scanning	Yes	Yes	Yes
Ethical Hacking (Servers)		Yes	Yes
Ethical Hacking (Workstations)		Yes*	Yes
Detective Control Capabilities			Yes
Vulnerability Impact Analysis		Yes*	Yes
Threat Analysis Reporting	Yes*	Yes	Yes
Follow Up Testing		Yes	Yes

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 in 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.

Thank You!

Questions?

Chris Wilkinson

Christopher.Wilkinson@crowe.com

Cell: 219.308.8980

Kiel Murray

Kiel.Murray@crowe.com

Cell: 814.450.2800

John Kurkowski

John.Kurkowski@crowe.com

Cell: 312.560.1257

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. © 2018 Crowe LLP.