KLR

CYBER RISK: WHAT'S AT STAKE FOR YOUR BUSINESS?

Presented by

Daniel M. Andrea, CPA, CITP, CISA

Dan has over 30 years of experience in public accounting and specializes in the performance of forensic accounting and litigation support procedures, SOC examinations, internal accounting controls assessments and information technology consulting services.

CYBER RISK: WHAT’S AT STAKE FOR YOUR BUSINESS?

AGENDA

- CURRENT ENVIRONMENT
- CYBER RISK: CORPORATE GOVERNANCE IMPLICATIONS
- CYBER SECURITY: IMPLEMENTATION PROGRAM
- CYBER SECURITY: BEST PRACTICES – ESSENTIAL CONTROLS

KLR

CURRENT ENVIRONMENT

CURRENT ENVIRONMENT

62%

of all cyber attacks (approximately 4,000 per day) occur in small to mid-size businesses

60%

of small businesses that experience a cyber attack are out of business in **6 months**

690K

The average price for small businesses to clean up after a “hack” is **$690,000**

KLR

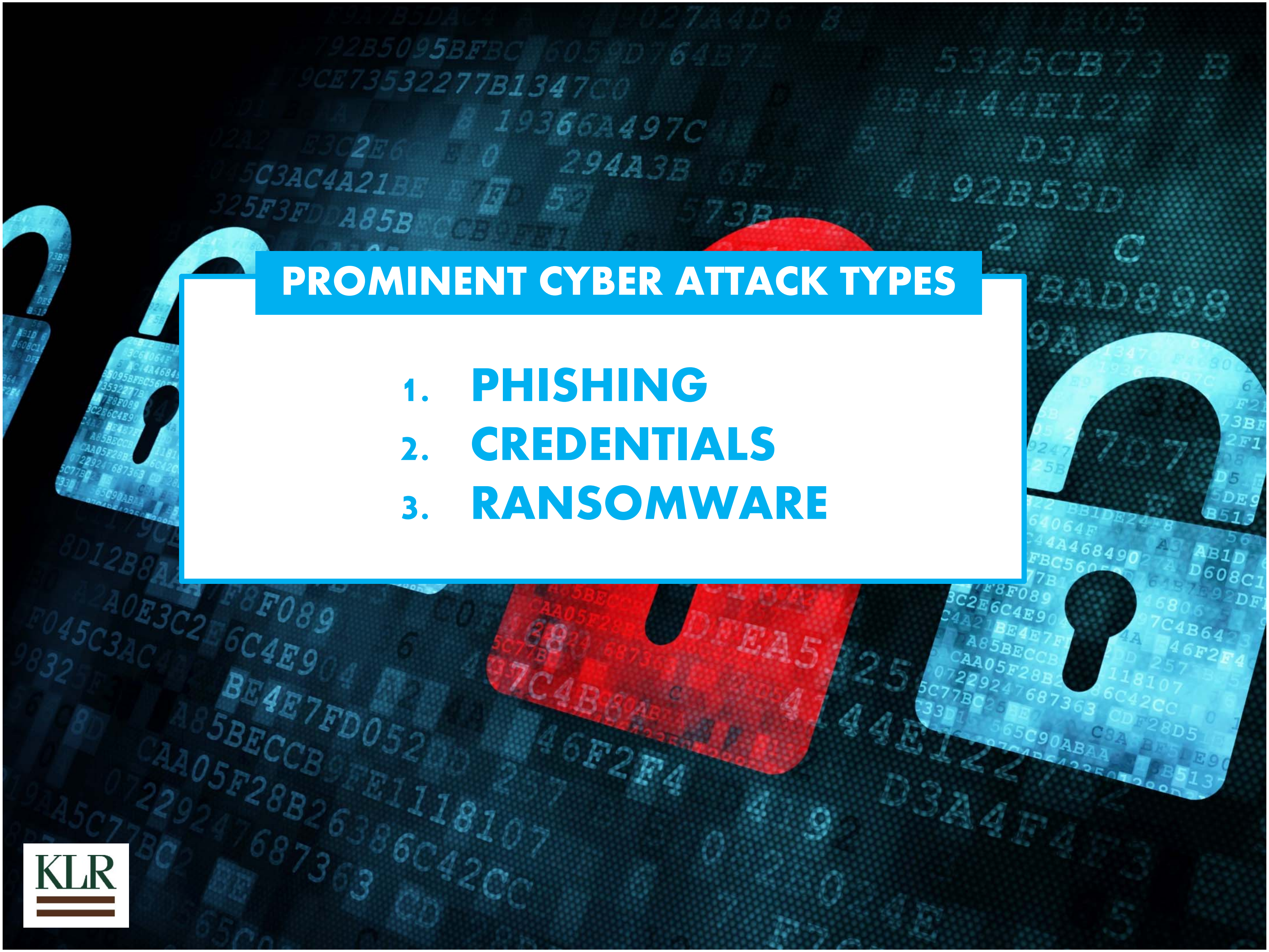
CURRENT ENVIRONMENT

The average time to identify that an event has occurred is **6 months** with an average time of **2 months** to contain the incident

75%

of companies breached learn from an outside party

KLR



PROMINENT CYBER ATTACK TYPES

1. **PHISHING**
2. **CREDENTIALS**
3. **RANSOMWARE**

CURRENT ENVIRONMENT

1 Phishing

A form of social engineering in which a message, typically an email, with a malicious attachment is sent to a victim with the intent of tricking the recipient to open an attachment.

13% of people are estimated to click on attachments.

CURRENT ENVIRONMENT

2 Credentials

Use of stolen information such as usernames and passwords. Standard mode of operation for organized criminal groups and state-affiliated attackers.

63% of confirmed data breaches involved weak, default or stolen passwords.

CURRENT ENVIRONMENT

3 Ransomware

A form of malware that encrypts files resident on the infected device and, in worst cases, attached file shares. Extortion demands follow.

KEY TAKEAWAYS

- Small to mid size business threats are real – not just the province of large corporations
- Various types of cyber attacks – phishing and ransomware are currently the attack de jour
- Credentials – we all need to do a better job of protecting our credentials (usernames and passwords) ; as well as not publicizing potentially exploitable information on social media

KLR

CYBER RISK: CORPORATE GOVERNANCE IMPLICATIONS

CYBER RISK: CORPORATE GOVERNANCE IMPLICATIONS

- Cyber Security is no longer chiefly the domain of CIOs, CISOs and IT Departments.
- Regulators (or interested third parties) increasingly expect that Board Members and Senior Managers have a sufficient grasp of cyber security core principles.

CYBER RISK: CORPORATE GOVERNANCE IMPLICATIONS

Threat is escalating (mobile devices, social media and the Internet of Things (IoT)).

Directors should ask questions about the types of scenarios that the company should plan for.

CYBER RISK: CORPORATE GOVERNANCE IMPLICATIONS

80%

of Directors discuss cyber security at most meetings but 66% lack confidence in their company's ability to protect itself.

CYBER RISK: CORPORATE GOVERNANCE IMPLICATIONS

41%

The biggest fear of 41% of Directors is brand damage due to loss of customers.

OTHER FEARS:

- cost of responding to breaches
- loss of competitive advantage
- regulatory and compliance violations

CYBER RISK: CORPORATE GOVERNANCE IMPLICATIONS

Awareness | Governance | Systems | Process | Strategy

Cyber Defense should incorporate these five themes

KLR

KEY TAKEAWAYS

- Not just an IT issue
- Senior Management needs to take an active role
- Unavoidable – Regulators and Interested 3rd parties are mandating policies and procedures to protect

KLR

CYBER SECURITY: IMPLEMENTATION PROGRAM

CYBER SECURITY: IMPLEMENTATION PROGRAM

Overview

1. Conduct a Risk Assessment
2. Build an Incident Response Team (“IRT”)
3. Share Information
4. Test the Incident Response Plan
5. Satisfy Legal Obligations

CYBER SECURITY: IMPLEMENTATION PROGRAM

1 Risk Assessment

NIST Framework has 5 elements ("functions")

- Identify
- Protect
- Detect
- Respond
- Recover

CYBER SECURITY:
IMPLEMENTATION PROGRAM

1 Risk Assessment

- Inventory of Systems
- Risk Assessment
- Implement measures to eliminate/mitigate risks
- Implement measures to detect potential incidents

CYBER SECURITY: IMPLEMENTATION PROGRAM

2 Build an IRT

- Comprised of All Key Stakeholders (internal/external)
- Define Incident Scenarios
- Build an Incident Response Plan ("IRP")

CYBER SECURITY: IMPLEMENTATION PROGRAM

3 Share Information

- Subscribe/Get Involved in Industry Groups
- Stay current on latest threats
- Modify Risk Assessment and IRP as appropriate
- Remediation

KLR

CYBER SECURITY: IMPLEMENTATION PROGRAM

4 Test the IRP

- Should be done at least annually
- Build realistic scenarios based upon Risk Assessment
- Conduct test
- Conduct Post-Mortem ("lessons learned")
- Modify IRP and Risk Assessment as appropriate

CYBER SECURITY:
IMPLEMENTATION PROGRAM

5 Satisfy Legal Obligations

- Know the laws at the federal, state and local jurisdiction relevant to you
- Consider cyber insurance

KLR

CYBER SECURITY: BEST PRACTICES

CYBER SECURITY: BEST PRACTICES

Essential Controls
TECHNICAL

1. Establish Technical Controls based upon the following Security Framework:
   - Enterprise Security
   - Endpoint Security
   - Data Security
   - Monitoring and Testing
   - Security Review and Evaluation

2. Controls should be established after the Risk Assessment

CYBER SECURITY: BEST PRACTICES

Enterprise Security

- Firewalls
- Intrusion Detection/Intrusion Prevention
- Network Segmentation
- DMZ
- Multi-Factor Authentication into the environment

KLR

CYBER SECURITY: BEST PRACTICES

Endpoint Security

- Antivirus/Anti-Malware
- Patch Management
- Data Loss Prevention ("DLP")
- Encryption
- Mobile Device Management ("MDM")

CYBER SECURITY: BEST PRACTICES

Data Security

- Access Controls
- Encryption
- File Access Monitor (“FAM”)
- Segmentation

CYBER SECURITY:
BEST PRACTICES

Monitoring and Testing

- Vulnerability and Penetration Testing
- Security Information and Event Management ("SIEM")
- Internal Scans

KLR

CYBER SECURITY: BEST PRACTICES

Security Review & Evaluation

- Quarterly Access Review
- Social Engineering Testing
- 3rd Party Examinations/Audits

KLR

CYBER SECURITY: BEST PRACTICES

Essential Controls

NON-TECHNICAL

- Continuous **USER EDUCATION**
- Security Awareness Training
- Robust Policies and Procedures with annual user attestation
- Limit Removable Media
- Limit Remote Access
- Password vs Passphrase policies
- Administrative Privilege Control

KLR

KEY TAKEAWAYS

- Not an IT issue – it's an Enterprise Issue
- Not "If" but "When"
- Start your Risk Assessment Today
- Understand what you are trying to protect
- Implement technical controls based upon the Risk Assessment
- Training, Training, Training

Let’s Connect

✉ dandrea@KahnLitwin.com

☎ 888-KLR-8557

KahnLitwin.com

KLR

BOSTON | NEWPORT | PROVIDENCE | SHANGHAI | WALTHAM
KAHNLITWIN.COM