Contractor

Cyber Law?
What is Cyber Security?

Definition

Measures taken to protect computers or computer systems against unauthorized access or attack

This can involve attacks against both computers as well as critical technology infrastructure
What is Cyber Security?

Three Key Elements in Cyber Security

- Prevention
- Detection
- Response
What is Cyber Security?

C.I.A. Triangle – Confidentiality, Integrity & Availability

Confidentiality: The principle that objects are not disclosed to unauthorized subjects.

Integrity: The principle that objects retain their veracity and are intentionally modified by authorized subjects only.

Availability: The principle that authorized subjects are granted timely access to objects with sufficient bandwidth to perform the desired interaction.
What is the Threat to Construction & Real Estate?

- Building Information Modeling and Virtual Project Management Have Increased Vulnerability.
What is the Threat to Construction & Real Estate?

- Increasing Phishing and Ransomware Attacks Reported Against Construction Industries.
What is the Threat to Construction & Real Estate?

- Highest Percentage of Phishing Attacks, Including Spam, Went to Construction-Related Industries last year.
What is the Threat to Construction & Real Estate?

- 50% of Real Estate Industry Says Their Organizations are not Adequately Prepared to Mitigate Cyber Security Risks.
What is the Threat to Construction & Real Estate?

- 30% of Real Estate Companies with One or More Properties Have Experienced a Cyber Security Event in the Last 2 Years.
Most Common Targets Were Customer Records, Employee Records and Physical Assets.
What is the Threat to Construction & Real Estate?

- Ex-Employees are Responsible for Over 1/3 of All Fraud Cases.
What is the Threat to Small Businesses?

- I’m a Small Fish – They Won’t Go After Me!
What is the Threat to Small Businesses?

- 62% of Larger Companies say they are Treating Response to Cyber Security Incidents as a High Priority.

Only 47% of Smaller Companies say the Same Thing.
What is the Threat to Small Businesses?

- The Cost Per Incident Per Record Released is the Same for Small and Large Companies.
What is the Threat to Small Businesses?

Two Primary Reasons Hackers Go After Small Businesses:

1. Small Businesses are Many and are a Ripe Market for Exploitation.
2. Larger Enterprises Have Already Enhanced Their Security.
What is the Threat to Small Businesses?

- Lower Costs of Computing Power Allow Bad Actors to Develop Malware that Permits More Sophisticated Attacks with Greater Frequency.
What is the Threat to Small Businesses?

• 43% of All Breaches Hit Companies with fewer than 250 Employees.
What is the Threat to Small Businesses?

- 60% of Small Businesses Hit with a Cyber Security Breach Go Out of Business in Six Months!
What is the Growing Threat to Everyone?

- 91% of Organizations Experience at Least One Cyber Security Incident in the Last Year.
• 81% of Respondents that were utilizing cyber threat intelligence (CTI) as a means of prevention, detection and response to cyber attacks believed their organizations had an increased ability to prevent and detect cyber security intrusions.
Sources and Types of Threats

Who Are Initiating the Attacks?

State Actors

Cyber Criminals
Internal Threats

48% of breaches caused by negligent and malicious insiders.

Malicious insiders have the highest annualized cost.

Malicious insiders take the longest to resolve.
Causes of Internal Threats?

- Lack of Diligence in Hiring
- Lack of Training
- Lack of Employee Monitoring
- Lack of Guarding from Former Employees
Why Internal Threats?

- Revenge, mischief, or vandalism
- Steal data, confidential information, or trade secrets for personal gain/new employment
- Nonmalicious transfers to personal accounts/devices during employment
- Embezzlement/Money
Common System Vulnerabilities

- Unsecured Communications
- Mismanaged User Access Credentials
- Unsecured Configurations
- Unpatched Vulnerability
Sources and Types of Threats

Types of Attacks

- Point of Sale Intrusions
- Phishing Attacks
- Password Attacks
- Man in the Middle
- Drive-By Download
- Malvertising
- Rogue Security Software
- Theft of Laptops or Mobile Devices
- Ransomware
In the first quarter of 2019, a 195% increase in ransomware attacks were detected.

SamSam Ransomware is used against most organizations. This typically uses an RSA 2048 encryption. (The average desktop would take 6.4 quadrillion years to crack the code).

The number of companies experiencing ransomware attacks has tripled over the last two years.

This is a very difficult situation and many organizations are paying. Most notably the City of Atlanta did not and spent $17 million in mitigation activities.

Back-ups are a challenge because the virus has a dwell time and could also be put in the back-up.
Sources and Types of Threats

What About The Cloud?

- Internal
- Hybrid
- External
Sources and Types of Threats

External Clouds

• **Due Diligence is Key!**
  • Understanding the external server’s disaster and recovery systems
  • Employee security policies
  • Protection of data

• **Cloud Certifications:**
  • National Institute of Standards and Technology (NIST)
  • Statement of Standards for Attestation Engagements No. 16 (SSAE16)
  • Service Organization Controls (SOC) 2 Type II
  • ISO 27001

• **Ignore at Peril**
  • Failure to use due diligence may violate state and/or federal law, including those required under Gramm Leach Billey Act (GLBA) and/or Health Insurance Portability and Accountability Act (HIPAA)
Legal Landscape

Legal Standard For Cyber Protection

- Gramm Leach Billey Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Fair Credit Reporting Act (FRCA)
- Children’s Online Privacy and Protection Act (COPPA)
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
- Telephone Consumer Protection Act (TCPA)
- Telemarketing Consumer Fraud and Abuse Prevention Act, the Deceptive Mail Prevention and Enforcement Act and the Computer Fraud and Abuse Act (CFAA)
- Federal Trade Commission (FTC)
- Written Information Security Program (WISP)
Regulatory Fines and Sanctions

- Double Whammy
Regulatory Fines and Sanctions

- Double Whammy
- Fines and Penalties
  - FTC
  - SEC
  - FINRA
  - PCI DSS
  - OCR
  - Justice Department
Board Exposure

- Boards need to approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue. (See Details in Written Materials.)
Limiting the Risk

Contracting to Limit the Threat

- Breaches by Vendors
- Increases Costs
- System Requirements/Certifications
- Indemnity Provisions
Limiting the Risk

Insurance
Capital and Administrative Investment

- Physical Security of Hardware
- Network Security
- Adopting a Risk Security Framework
- Training
Limiting the Risk

Risk Assessment

WHY YOU NEED IT AND HOW TO GET STARTED
Limiting the Risk

Incident Response Plan

Incorporating Risk Assessment
Limiting the Risk

Incident Response Plan

Establishing a Team
Limiting the Risk

Incident Response Plan

Process
Limiting the Risk

Incident Response Plan

Technology
Limiting the Risk

Incident Response Plan

Testing
Limiting the Risk

Incident Response Plan

Revise and Improve
Limiting the Risk

Incident Response Plan

Post-Incident Remediation
Responding to a Breach

Technical/System Phases of an Incident Response

- Preparation
- Detection & Analysis
- Containment, Eradication & Recovery
- Post-Incident Activity
Responding to a Breach

Look to Your Incident Response Plan
Look to Your Incident Response Plan

Act Immediately to Limit Damage and Mitigate Exposure and Expense
Responding to a Breach

Look to Your Incident Response Plan
Act Immediately to Limit Damage and Mitigate Exposure and Expense
Determine if Internal or External Attack
Responding to a Breach

Look to Your Incident Response Plan
Act Immediately to Limit Damage and Mitigate Exposure and Expense
Determine if Internal or External Attack

Preservation of Evidence
Engage Outside Legal Counsel
Responding to a Breach

Look to Your Incident Response Plan
Act Immediately to Limit Damage and Mitigate Exposure and Expense
Determine if Internal or External Attack
Preservation of Evidence
Engage Outside Legal Counsel
Retain an Expert to Provide an Objective and Outside View
Responding to a Breach

Look to Your Incident Response Plan
Act Immediately to Limit Damage and Mitigate Exposure and Expense
Determine if Internal or External Attack
Preservation of Evidence
Engage Outside Legal Counsel
Retain an Expert to Provide an Objective and Outside View

Determine Whether Law Enforcement Needs to be Notified
Responding to a Breach

Look to Your Incident Response Plan
Act Immediately to Limit Damage and Mitigate Exposure and Expense
Determine if Internal or External Attack
Preservation of Evidence
Engage Outside Legal Counsel
Retain an Expert to Provide an Objective and Outside View
Determine Whether Law Enforcement Needs to be Notified
Determine Whether a Public Announcement is Required
Responding to a Breach

Look to Your Incident Response Plan
Act Immediately to Limit Damage and Mitigate Exposure and Expense
Determine if Internal or External Attack
Preservation of Evidence
Engage Outside Legal Counsel
Retain an Expert to Provide an Objective and Outside View
Determine Whether Law Enforcement Needs to be Notified
Determine Whether a Public Announcement is Required
Determine Whether Notification to an Insurer is Required
Responding to a Breach

Look to Your Incident Response Plan
Act Immediately to Limit Damage and Mitigate Exposure and Expense
Determine if Internal or External Attack
Preservation of Evidence
Engage Outside Legal Counsel
Retain an Expert to Provide an Objective and Outside View
Determine Whether Law Enforcement Needs to be Notified
Determine Whether a Public Announcement is Required
Determine Whether Notification to an Insurer is Required
Examine Software and Hardware to Determine the Network is “Clean”
Responding to a Breach

Look to Your Incident Response Plan
Act Immediately to Limit Damage and Mitigate Exposure and Expense
Determine if Internal or External Attack
Preservation of Evidence
Engage Outside Legal Counsel
Retain an Expert to Provide an Objective and Outside View
Determine Whether Law Enforcement Needs to be Notified
Determine Whether a Public Announcement is Required
Determine Whether Notification to an Insurer is Required
Examine Software and Hardware to Determine the Network is “Clean”
Engagement in a Forensic Examination of the Causes of What Occurred and Avoid a Repeat
Responding to Social Media Attacks
Responding to Social Media Attacks

PROACTIVE MEASURES

Manage and Monitor  (THERE IS NO HALF WAY)
Responding to Social Media Attacks

PROACTIVE MEASURES

Manage and Monitor (THERE IS NO HALF WAY)
Know What Is and Is Not a Crisis.
Responding to Social Media Attacks

PROACTIVE MEASURES

Manage and Monitor  (THERE IS NO HALF WAY)
Know What Is and Is Not a Crisis.

Set Up a Listening Program
Responding to Social Media Attacks

COMBATTING AN ATTACK

STEP 1

Do Not Act Impulsively or Retaliate
Responding to Social Media Attacks

COMBATTING AN ATTACK

STEP 1
Do Not Act Impulsively or Retaliate

STEP 2
Identify the Nature, Source and Extent of the Attack
Responding to Social Media Attacks

COMBATTING AN ATTACK

Do Not Act Impulsively or Retaliate

Identify the Nature, Source and Extent of the Attack

Evaluate Potential Responses:
1. Contact Media Platform to Remove
2. Contact Known Attacker Directly
3. Reaching Out to Unknown Attacker
4. Issue Public Statement
COMBATTING AN ATTACK

STEP 1
Do Not Act Impulsively or Retaliate

STEP 2
Identify the Nature, Source and Extent of the Attack

STEP 3
Evaluate Potential Responses

STEP 4
Legal Action

Responding to Social Media Attacks
10+ Tips To Staying Safe

Invest In Active Protective Software

- Firewall
- Detection Software
10+ Tips To Staying Safe

Invest In Active Protective Software

Secure Your Networks

Wi-Fi
Router
10+ Tips To Staying Safe

Invest In Active Protective Software
Secure Your Networks
Protect Personal Information

Policies
Transmission
Invest In Active Protective Software
Secure Your Networks
Protect Personal Information

Employee Training and Accountability

- Educate Employees About Cyber Threats and Hold Them Accountable
- Educate Employees to Avoid Phishing Attacks
- Prohibit Employees From Inserting **USB Drives** into Network Computers Without Checking for Malware First
10+ Tips To Staying Safe

A Word About USB Drives
10+ Tips To Staying Safe

- Invest In Active Protective Software
- Secure Your Networks
- Protect Personal Information
- Employee Training and Accountability
- **Strong Passwords**
  - Passwords
  - Two-Factor Authentication
Invest In Active Protective Software
Secure Your Networks
Protect Personal Information
Employee Training and Accountability
Strong Passwords

Employ Best Practices on Payment Cards
10+ Tips To Staying Safe

Invest In Active Protective Software
Secure Your Networks
Protect Personal Information
Employee Training and Accountability
Strong Passwords
Employ Best Practices on Payment Cards
Backup Data
10+ Tips To Staying Safe

Invest In Active Protective Software
Secure Your Networks
Protect Personal Information
Employee Training and Accountability
Strong Passwords
Employ Best Practices on Payment Cards
Backup Data
Control Physical Access to Computers & Network Components
Invest In Active Protective Software
Secure Your Networks
Protect Personal Information
Employee Training and Accountability
Strong Passwords
Employ Best Practices on Payment Cards
Backup Data
Control Physical Access to Computers & Network Components
Create a Mobile Device Action Plan

10+ Tips To Staying Safe
10+ Tips To Staying Safe

Invest In Active Protective Software
Secure Your Networks
Protect Personal Information
Employee Training and Accountability
Strong Passwords
Employ Best Practices on Payment Cards
Backup Data
Control Physical Access to Computers & Network Components
Create a Mobile Device Action Plan
Website Protection
Thank You