Welcome
Cyber Risk is Real
Continuity Planning

Dena Johnson, MBA, EDFP
Djohnson@PayneWest.com
(406) 238 1992

Chantel Sparovic
Csparovic@PayneWest.com
(406) 238 1913

Richard Stone, Cyber Underwriter
Travelers Insurance

PayneWest INSURANCE
A Marsh & McLennan Agency LLC company
Thank you to our host & sponsor!
Cyber-crime
Cyber risk – exposures
Cyber mitigation
Incident response team/plan
Incident recovery
Small Businesses need protection

Small Does NOT = Safe

Small Businesses are Vulnerable Too

72% of Cyber Attacks affect companies with less than 100 employees.

50% of small businesses think they are too small to be hacked.

The average amount it takes a small business to recover from a cyber attack is $188,242.

Source: Cyber Security Forum for Senior Executives
Doing business looks different...
What is cyber-crime?
cybercrime

/ˈsɪbərˌkrɪm/

noun
noun: cyber-crime

criminal activities carried out by means of computers or the internet.

Definitions from Oxford Languages
Types of cyber-crime
The Most Common Types of Cyber Crime

Number of Americans who fell victim to the following types of internet crime in 2020:

- Phishing/Vishing/Smishing: 241,342
- Non-Payment/Non-Delivery: 108,869
- Extortion: 76,741
- Personal Data Breach: 45,330
- Identity Theft: 43,330
- Spoofing: 28,218
- Misrepresentation: 24,276
- Confidence/Romance Fraud: 23,751

Total victim losses from the listed crimes: $1.64 billion

Source: The FBI’s Internet Crime Complaint Center

statista
YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.) Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.
You have 72 hours to pay the fine, otherwise you will be arrested.
You must pay the fine through
To pay the fine, you should enter the digits resulting code, which is located on the back of your in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
PHISHING

Your mailbox is almost full.

4025 MB 4096 MB

Click here to permanently increase your mailbox size to 8192 MB.
VISHING
SMISHING
Unintentional & Intentional employee disclosure
Point of Sale
Bring your own device (BYOD)
Website risk
Cyber-attacks are real
How well do you know your business’ cyber exposures?

1. Does your business retain physical or electronic records of employees or other third parties with any of the following?
   a. Social security numbers
   b. Drivers’ license information
   c. Tax identification numbers
   d. Birth dates
   e. Medical/health records
   f. Court records
   g. Police records
   h. Banking information (checking/savings accounts)
   i. Email addresses or home addresses

**FACT:** If you checked any of the above, your organization is in control of “Personally Identifiable Information,” and therefore, required to protect that data subject to State and Federal privacy and data breach notification laws.
Work-anywhere – is normal (no longer new)
Liabilities to third parties:
• Employees, vendors, suppliers, public arising out of breach of information or pass-through malware
• Media Liability

Legal Defense and Investigation
• Costs incurred to defend claims or research obligations under laws of multiple jurisdictions

Forensics
• Source of breach/loss, confirmation of quarantine or disposal

Regulatory Fines and Defense
• HIPAA, GDPR, CCPA, state statutes

Business Interruption/Expense to resume pre-breach operations
• Loss of business while operations suspended or impaired due to breach

Data Restoration
• Cost to recover, retrieve or reinstate data lost as result of breach

Physical Damage
• Cost to replace servers and other computer equipment

Ransomware
• Cost of ransom, forensics, or data restoration

Reputational Damage
• Loss of business due to public perception of data security
• Public Relations & Crisis Management

Other/Emerging
• Funds transfer type frauds – Social engineering or invoice manipulation
• Bodily Injury or Property Damage

“The Unknown”
• aka Silent Cyber

Exposures
The Greatest Threats To The U.S. According To Americans

The most critical threats to the U.S. over the next decade, as cited by U.S. adults

<table>
<thead>
<tr>
<th>Threat</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyberterrorism/use of computers to cause disruption/fear in society</td>
<td>82%</td>
</tr>
<tr>
<td>Development of nuclear weapons by North Korea</td>
<td>77%</td>
</tr>
<tr>
<td>Development of nuclear weapons by Iran</td>
<td>75%</td>
</tr>
<tr>
<td>International terrorism</td>
<td>72%</td>
</tr>
<tr>
<td>Spread of infectious diseases throughout the world</td>
<td>72%</td>
</tr>
<tr>
<td>The economic power of China</td>
<td>63%</td>
</tr>
<tr>
<td>Global warming or climate change</td>
<td>58%</td>
</tr>
<tr>
<td>Large numbers of immigrants entering the U.S. illegally</td>
<td>46%</td>
</tr>
<tr>
<td>The military power of Russia</td>
<td>44%</td>
</tr>
<tr>
<td>Conflict between the Israelis and Palestinians</td>
<td>32%</td>
</tr>
<tr>
<td>Conflict between China and Taiwan</td>
<td>30%</td>
</tr>
</tbody>
</table>

n=1,021 adults (Feb 3-18, 2021)
Source: Gallup

Statista
What is cyber-security?
Types of Cyber-security – humans!

95% of cybersecurity breaches are caused by human error.

Cybint
Education & Training
What is MFA or 2FA?
What is Multifactor Authentication (MFA)?

The use of two or more authentication factors. MFA is successfully enabled when at least two of these categories of identification are required in order to successfully verify a user’s identity *prior* to granting access.

1. SOMETHING YOU KNOW
2. SOMETHING YOU HAVE
3. SOMETHING YOU ARE
Why is MFA critical?

99.9% of account compromise attacks can be blocked by MFA\(^1\)

94% of ransomware victims investigated did not use MFA\(^2\)
What should be protected with MFA?

- Remote Network Access
- Privileged/ Administrative Access
- Remote Access to Email
MFA Example
LastPass MFA is a smarter way to authenticate

Leverage biometric and contextual factors to better protect your business while simplifying the employee login experience.

Start a Trial
Contact Us  Buy Now

Leverage biometric and contextual factors to better protect your business while offering a passwordless user experience for employees.
Encryption = Protection
Cloud
Anti-virus software

Best Device-to-Cloud CYBERSECURITY

- Endpoint Security: Defend your endpoints with a single console and integrated controls.
- Cloud Security: Secure any cloud; protect your data wherever it goes.
- Threat Intelligence: Explore unparalleled threat data from our AI and Machine Learning.

Discover How Latest Threat Report
Rocky Mountain Region's Most Trusted IT Provider

Discover the process trusted by IT leaders to accelerate core business objectives while securing organizational assets.
What is Cyber Insurance?
INCIDENT RESPONSE TEAM

COMPUTER FORENSICS
A forensic IT team assesses the damage to determine what was compromised. How did they get access? Can we get it back?

LEGAL
Notification costs, regulatory compliance, negotiations with ransom demand

ACCOUNTING
Quantify the loss in revenue

BREACH COACH
<table>
<thead>
<tr>
<th>CREDIT MONITORING</th>
<th>DATA RECOVERY FIRM</th>
<th>PUBLIC RELATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IT experts to get your systems back up and running after you get the encryption key</td>
<td>Manage professional communications (damage control) related to the incident</td>
</tr>
</tbody>
</table>
### STATE OF THE CYBER MARKET

<table>
<thead>
<tr>
<th>PREMIUMS</th>
<th>DEDUCTIBLES</th>
<th>NEW MARKETS</th>
<th>CONTROLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upward pressure on premiums. Typically see 5% - 30% increases on renewals.</td>
<td>First time we’ve seen deductibles increasing without an option to buy the deductible down</td>
<td>new carriers entering this market has slowed down. Lots of new players in the Cyber Insurance Space.</td>
<td>Strict Ransomware applications requiring certain controls including dual authentication. Scanning networks for weakness as part of the underwriting process</td>
</tr>
</tbody>
</table>

**TRENDS**
DATA SECURITY: Contractor has developed and implemented a comprehensive information security program that includes controls to ensure security of Data (firewalls, anti-virus software, two-factor authentication, awareness training)

INFORMATION SECURITY TRAINING: Contractors with electronic access to any network or information system owned by the Owner/GC. Only authorized and trained persons

SECURITY INCIDENT RESPONSE PLAN: Contractor shall develop and implement a “response plan”, which shall be policies and procedures to address Security Incidents.

NOTIFICATION: Any unauthorized use or access, penetration, or security breach must be reported and Contractor shall be required to remedy and mitigate any damages, losses, or expenses caused by a breach in the Contractors security systems.

CYBER LIABILITY: Contractor shall carry a Cyber Liability Policy with limits of not less than $1,000,000. Coverage must include a Cyber Deception Fraud limit of at least $100,000
Cyber security S W O T (audit)
No magic bubble
THANK YOU

Questions?

Dena Johnson, MBA, EDFP
Dljohnson@PayneWest.com
(406) 238 1992

Chantel Sparovic
Csparovic@PayneWest.com
(406) 238 1913

PayneWest
INSURANCE

A Marsh & McLennan Agency LLC company

Richard Stone, Cyber Underwriter
Travelers Insurance