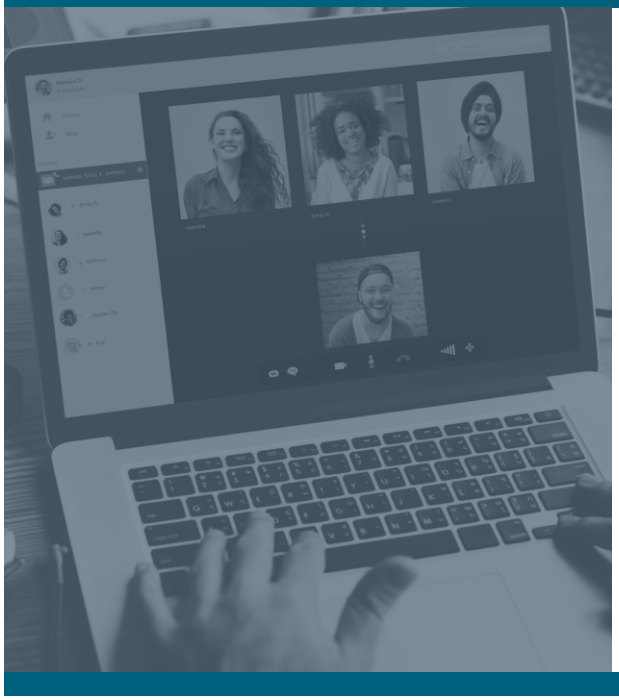


Cybersecurity: How Vulnerable are You?

1

What is at risk?

Your Reputation	Financial Performance	Regulatory Environment

2

Questions to discuss with your IT team

3

E-Mail Security

Do we strictly enforce Sender Policy Framework (SPF) on incoming e-mails?

- *Why is this important?* Checks for all inbound email messages, verifying the validity of sending organizations. Filter all inbound messages for malicious content including executables, macro-enabled documents and links to malicious sites.

Can our users access email through a web app on a non-corporate device? If so, do we have multi-factor authentication (MFA) enabled?

- *Why is this important?* MFA is two authenticating factors to verify the identity of an individual. For example, password and app or password and biometric identification such as your fingerprint.

Do we use Office 365? Do we use the o365 Advanced Threat Protection add-on?

- *Why is this important? A* cloud-based email filtering service that protects you from malware, ransomware, harmful links, and more. It protects you from malicious URLs in email or Office documents.

4

4

Internal Security

Do we use endpoint protection products (EPP) and endpoint detection response (EDR) across our enterprise?

- *Why is this important?* EPP is traditional anti-malware scanning. EDR provides advanced capabilities like detecting and investigating security incidents, and ability to remediate endpoints to pre-infection state. It uses artificial intelligence.

Do we have end of life or end of support software? If so, is it segregated from the rest of the network? If not, what mitigating steps are we taking?

- *Why is this an issue?* Security vulnerabilities concerns since it can no longer be updated.

Do we use MFA to protect privileged user accounts and remote access?

- *Why is this important?* Additional protections for general users and. system access. Privileged access for critical assets (servers, end-points, applications, databases, etc.) and enforce MFA for remote access (VPN, externally facing applications, etc).

5

Back Up and Recovery Policy

Are our backups encrypted?

- *Why is this important?* If backups aren't encrypted then unauthorized users can access the data.

Are our backups kept separate from our network/ offline, or in cloud service designed for this purpose?

- *Why is this an issue?* Protect integrity of backups in the event your network is compromised by malware.

Have we tested the successful restoration and recovery of key service configurations and data from backups in the last 6 months? What is our recovery time objective?

- *Why is this important?* Critical to business continuity and how long restoration may take.

6

Back Up and Recovery Policy

Are we able to test the integrity of backups prior to restoration to be confident it is free from malware?

Does our incident response plan (IRP) specifically address ransomware?

- *Why is this important?* IRP is the playbook if an incident occurs. Ransomware is one of the most common claims we see and it's important to address in your IRP. It identifies the escalation steps, decision makers, and when to engage outside resources, etc.

Have we carried out a table-top exercise to test our IRP implementation?

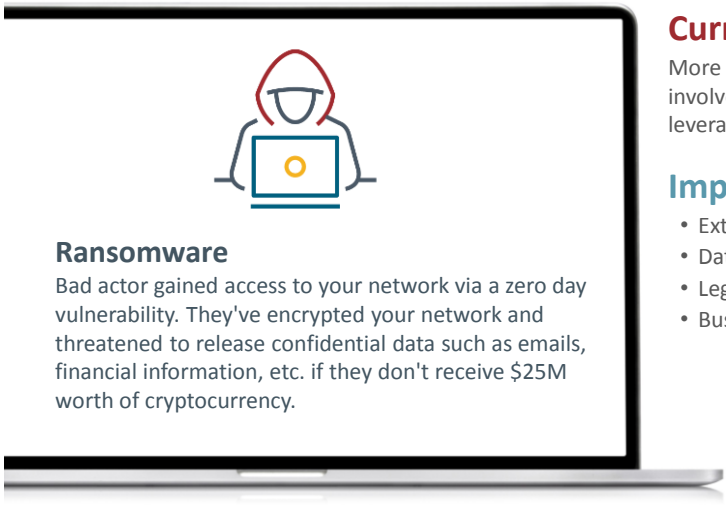
- *Why is this important?* Similar to fire drills, it's important to test the plan.

7

Potential Risk Area - Cyber Extortion overview

8

Cyber Extortion



Ransomware

Bad actor gained access to your network via a zero day vulnerability. They've encrypted your network and threatened to release confidential data such as emails, financial information, etc. if they don't receive $25M worth of cryptocurrency.

Current Trend

More than 1 in 10 ransomware attacks in H1 2020 involved the theft of data, increasing the attackers' leverage and potential response costs. *Source: emisoft*

Impact on you

- Extortion demand
- Data restoration costs
- Legal, IT forensics and crisis management costs
- Business income loss due to downtime

9

9

Cyber Extortion – Bricking Coverage

Bricking Coverage

During a cyber-attack, physical equipment may be compromised, damaged, or rendered useless due to malware. Anything from a USB drive to a laptop or a server may be damaged so badly that it can no longer function as anything other than a brick. Bricking coverage may replace those items.

Source: https://www.oswaldcompanies.com/risk-hubs/cyber-risk/

Frequency

Typically occurs during ransomware events and property coverage may or may not respond

Impact on you

- Further complicates downtime
- Increased Cost/Expense

10

10

Risk Area – Cyber Terrorism / Network Liability / Cyber Crime

11

Cyber Terrorism / Network Liability / Cyber Crime

Current Trend

The SolarWinds incident is an example of this scenario.

According to the 2020 FBI's IC3 report, it was a record year with 791,790, with reported losses exceeding $4.1 billion.

Impact on your business

- Downtime
- Litigation due to transmission of malicious software to third parties
- Loss of funds due to social engineering

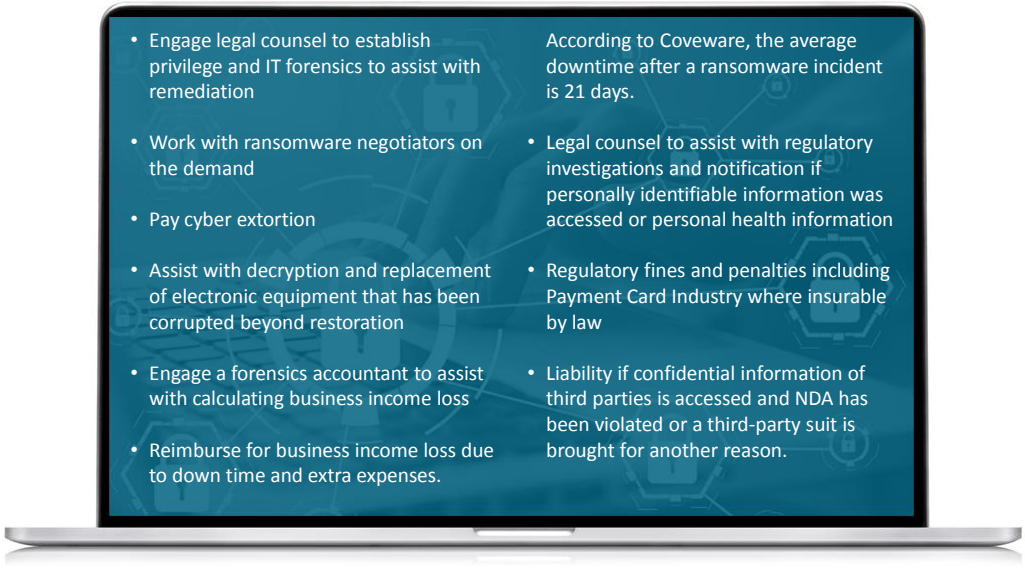
Typical cost range (Regulatory fines and liability):

- Average: $1.6M
- High: $2.2M

12

12

Cyber Liability Coverage Solution



13

13

Underwriting Changes

- Coinsurance up to 50%
- Rate increases from 40% to 100%
- New Exclusions
- Sublimiting cyber extortion, etc
- Limiting dependent business interruption
- Rigorous underwriting process

14

14

Cybersecurity Control Expectations

Protecting your company against ransomware

Minimum Protection	Stronger Protection	Best Protection
◆End-Point Protection (EPP) solution ◆Email tagging ◆Enforce strict Sender Policy Framework (SPF) ◆Multi Factor Authentication throughout network ◆Disable macros from automatically running ◆Patching cadence ◆Use Remote Desktop Gateway (RDG) or secure RDP behind a multi-factor authentication-enabled VPN. ◆Rehearsed incident response process plan ◆Back-up key systems and databases and stored offline ◆Educate your users ◆Firewalls	◆Secure baseline configuration ◆Filter web browsing traffic ◆Use of protective DNS ◆Manage privileged access effectively ◆Regularly test back-ups ◆Disconnect back-ups from network ◆Separately store unique back-up credentials	◆Endpoint Detection and Response (EDR) ◆Intelligent email evaluation ◆Centralized log monitoring ◆Subscription to external threat intelligence services ◆Encrypted back-ups ◆Network segmentation ◆Web isolation ◆Application permissions

15

15

CORE VALUES

Passion for Excellence

Integrity

Resourcefulness

Commitment to Community

taylor oswald

Women's Leadership Council oswald

oswald CLIMBS

PARTNERSHIPS & INITIATIVES

creating a diverse, equitable and inclusive culture at Oswald.

WHAT WE DO

STRATEGIC RISK MANAGEMENT

Property & Casualty

Employee Benefits & Health Management

Life Insurance

Retirement Plan Services

Personal Risk Management

AWARDS AND ACCOLADES

TOP WORK PLACES 2020 — 7th Consecutive Year — The Plain Dealer — cleveland.com

FORTUNE 100 BEST COMPANIES TO WORK FOR®

BUSINESS INSIDER GREAT PLACE TO WORK®

oswald UNIVERSITY

North Coast 99

400+

100% EMPLOYEE OWNED

with over 400 employee-owners and growing!

FOUNDED IN 1893

CLEVELAND HQ

One of the nation's largest independent insurance brokerage firms, with 7 offices spanning Ohio and Michigan.

Assurex GLOBAL

LOCAL SERVICE. GLOBAL SCALE.

Proud member of the world's largest association of privately held insurance brokers.

OswaldCompanies.com 1-855-4OSWALD

oswald

16