Cyber Risk
Huntington Insurance

Ashley Bauer, VP

Ransomware

Ransomware is a form of malware that **restricts the target from using their device or retrieving their files until a ransom is paid.** Normal functionality will not be restored by the perpetrator unless an untraceable fee is paid (instructions provided) within a designated period of time. In many cases, ransomware encrypts any files it can access, and the fraudster is the only one with the primary key that can successfully decrypt them. If the payment is made in the allotted period of time, the fraudster claims that they will decrypt the effected files. **Some ransomware demands can be appear to come from legitimate entities (i.e. FBI).**

Business Email Compromise

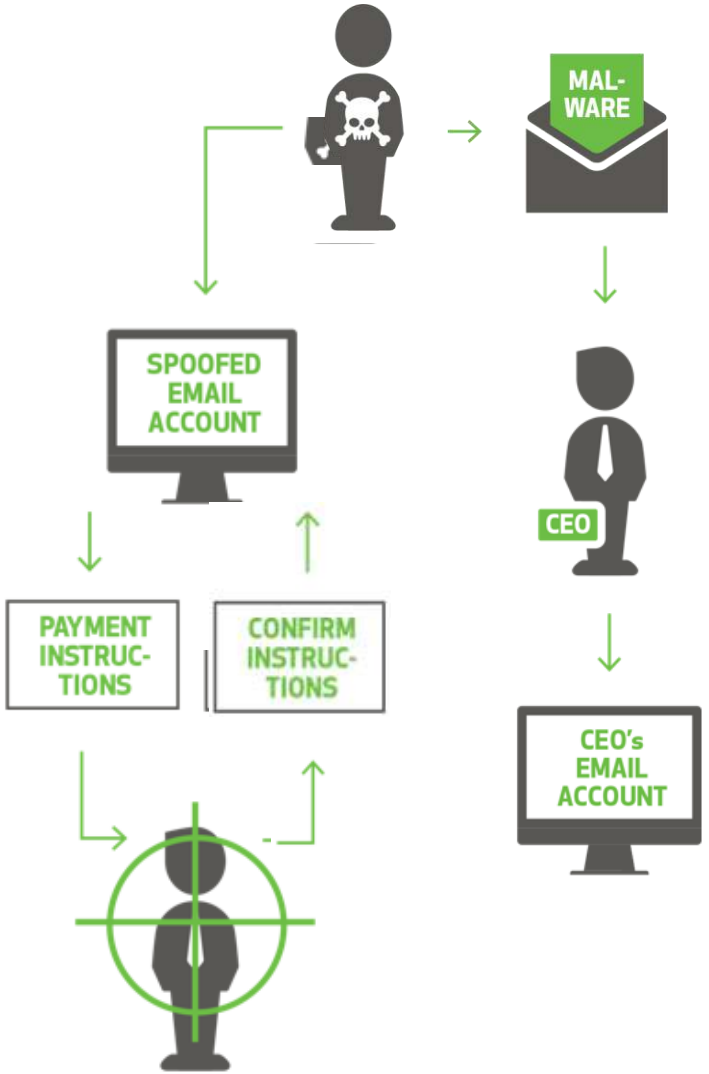
Fraudster uses spear phishing tactics to **compromise the email of a company's CEO**

Access to the CEO's email is acquired, and **the fraudster reviews all available info** (calendar, email history, language/signature/templates used, who executes monetary transactions, etc.)

A payment request is sent to an employee at the target company from an email account created by the fraudster that mirrors or closely resembles the CEO's email account

The **employee confirms the request via email** with the fraudster, who they believe to be the CEO

The employee, believing the request to be legitimate, **initiates the fraudulent payment**



Norton: Emerging Threats

The Cost of Cybercrimes

Internet crime victim losses in 2020:	**$4.2 billion**
The average cost of a ransomware attack:	**$1.85 million**
Global cybercrime damages per second:	**$190,000**
The average cost of cybercrime for organizations:	**$13 million**

Devices and Platforms at Risk

Reasons to worry about our favorite gadgets and online communities.

70% of online fraud is accomplished through mobile platforms.

3 in 5 U.S. gamers admit they worry gaming will become less secure.

53% of people distrust IoT devices to protect their privacy and handle their information.

34% of U.S. adults don't trust social media companies at all with safeguarding their data.

Source: RSA, Norton, Internet Society, Statista

Cyberattacks at a Glance

Ponder these prominent cybersecurity threats in recent years.

There was a 40% surge in global **ransomware** in 2020.

22% of consumers have detected **malware** on an internet-connected devices.

Phishing was the topmost internet crime reported to the FBI in 2020.

There was a 67% increase in **security breaches** between 2014 and 2019.

Instances of **stalkerware** increased by 20% from November 2020 to January 2021.

Social engineering is the most successful means to a data breach.

Source: SonicWall, Norton, FBI, Accenture, Verizon

https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

Cyber Threats top concern

Cyber threats are the top concern for U.S. business leaders, according to the 2021 Travelers Risk Index

- 59% of the 1,200 business leaders who participated in the national survey said they worry some or a great deal about cyber
  - Compared to medical cost inflation (53%)
  - Increasing employee benefit costs (53%)

- **Security breaches, system glitches** and **unauthorized access to bank accounts** are the top three cyber-specific business concerns

- More than 1 in 2 of companies believe it is inevitable they will be the victim of a data breach or cyberattack (including ransomware)

https://www.businesswire.com/news/home/20210929005518/en/Travelers-Risk-Index-Cyber-Ranks-as-the-Top-Business-Concern

Cyber Threats top concern

- Only 61% of participants reported feeling extremely or very confident in their company's cyber practices

- **Less than half of survey respondents have adopted basic preventive measures available to companies**, such as multifactor authentication

- One-fourth of participants said their company has been a cyber victim, with nearly half reporting that the event happened within the past 12 months.

We constantly work to raise awareness of the serious and costly consequences that cyber threats can pose," said Tim Francis, enterprise cyber lead at Travelers. “These survey results show that despite cyber risks being the top concern, too many companies are unprepared to deal with them. It's crucial that businesses take the necessary actions to protect their data and assets, especially with so many employees continuing to work remotely."

https://www.businesswire.com/news/home/20210929005518/en/Travelers-Risk-Index-Cyber-Ranks-as-the-Top-Business-Concern

Recent events with systemic loss potential

- **Blackbaud (2019)** – data breach of US software vendor impacting thousands of organizations
- **AWS Kinesis (2020)** – leading cloud hosting provider experienced a 17-hour outage
- **Gmail (2020)** – top three email service provider experienced an outage for over two hours
- **SolarWinds (2020)** – ubiquitous network monitoring tool experienced a software supply chain attack
- **FireEye, Malwarebytes, Emisoft, Mimecast (2020)** – among other large security firms all targeted by sophisticated actors
- **Microsoft Exchange (2021)** – four zero-day vulnerabilities in Microsoft Exchange Server are being actively exploited by a state-sponsored threat group and appear to have been adopted by other cyberattackers in widespread attacks
- **Colonial Pipeline (2021) -** single ransomware encounter impacting an outage to infrastructure on US East Coast
- **PrinterNightmare (2021)** – zero day vulnerability, and exploit, with scale of exposure across MSFT OS
- **Kaseya (2021) –**SPoF supply-chain attack leading to widespread ransomware encounters originating from users of Kaseya VSA (primarily MSP/MSSPs)
- **Accellion, Log4J, Kronos, ….**

CHUBB

Huntington

2022 P&C Market Forecast

2022 Market Outlook Forecast Trends

Price forecasts are based on industry reports for individual lines of insurance. Forecasts are subject to change and are not a guarantee of premium rates. Insurance premiums are determined by a multitude of factors and differ per organization. These forecasts should be viewed as general information and not insurance or legal advice.

Line of Coverage	Price Forecast
Commercial property	+5% to +15%
General liability	+2.5% to +15%
Commercial auto	+10% to +25%
Workers' compensation	-2% to +5%
Cyber liability	+15% to +50%
Directors and officers liability	Public entities: +5% to +25% or more Private/nonprofit entities: +5% to 35%
Employment practices liability	+10% to +25%

Price forecasts are based on industry reports for individual lines of insurance. Forecasts are subject to change and

Advisen News

US cyber pricing skyrockets an average 130% in Q4: Marsh — **Insurance Market**

Alex Zank and Erin Ayers, Advisen

Cyber insurance pricing again shot up in the fourth quarter of 2021, rising 130% in the U.S., up from an average increase of 96% in Q3, according to Marsh's Global Insurance Market Index.

Cyber Exposures

- How to identify cyber risk
  - *A network*
  - *Employees*
  - *System access to the internet*
  - *Sensitive Data Storage (financial, medical and/or employee records)*
  - *Permitting vendors/suppliers to have access to network systems*
  - *Business continuity dependent on a particular system or vendor*
  - *Online sales and payment card processing (even if outsourced)*
  - *Online financial transactions including ACH and accounts payable functions*
  - *Contract requirements*

Cyber Discussion

Many of our clients are very concerned about cyber losses, how are you addressing your cyber risk?

There have been a lot of changes to cyber policies lately. Has your broker talked to you about this and how your coverage has changed?

- Coinsurance may be used for important coverage parts like ransomware, requiring you to pay for a portion of the loss in addition to your deductible
- Your full limits may not apply for losses caused by Widespread Cyber Events *(example: Microsoft Exchange and Solarwinds)* leaving you with less protection than you think
- The importance of coordinating coverage between Cyber, Crime and D&O policies to prevent gaps or overlaps

What is your insurance broker telling you to expect for your upcoming cyber insurance renewal?

Cyber Discussion

At Huntington we have an Insurance Executive Risk Practice with experts in Cyber.

In coordination with the fraud protection we offer you as a bank, we can work with our Insurance team to customize risk management solutions.

They can work with you to understand:

- The state of the cyber insurance market
- Your network security posture in relation to insurance company requirements
- Strategize on available insurance solutions

Would you like to set up a meeting with our team?