Cybersecurity

Emerging Cyber Threats

May 20, 2021

Presented by

Seth Johnson, CSRM - Risk Management Consultant, CIC

COMMUNITY INSURANCE CORPORATION

Cyber Liability

Security Industry Headlines

2014 | The Year Cyber Danger Doubled

2015 | The Year Data Breaches Became Intimate

2016 | The Year Hackers Stole The Show with a Cause

2017 | The Year Hurricanes Devastated the Land, Data and Trust

2018 | The Year Privacy Took Center Stage

2019 | The Year Ransomware Targeted State and Local Governments

2020 | The Year that Brought Two Pandemics

The Remote Threat Environment

- Attackers have been aware of remote work as a threat vector for some time
- Attackers are taking advantage of interest in and repercussions of COVID-19 to remain current
- The rapid shift to remote work has resulted in the growth of personal devices being used for business
- Home networks are not professionally managed
- Remote worker endpoint security
- Remote access technologies

Continued Escalation of Targeted Ransomware Attacks

- Ransomware is a cyberattack that combines extortion with **mal**icious soft**ware** (**malware**)
- Ransomware typically falls into two main categories:
  - Locker ransomware
  - Crypto ransomware
- These attacks are widespread because:
  - They are highly profitable for cybercriminals
  - They provide a mechanism for sabotaging an organization’s operations or infrastructure
  - Many individuals and organizations are vulnerable
- Ransomware as a service (RaaS) schemes

Phishing Gets More Sophisticated

- Phishing attacks are a kind of social engineering attack where the attacker generates a fraudulent email, text, phone call, direct message chat or website to trick a victim into surrendering sensitive information or into downloading malware.
- More attackers are using phishing strategies because they are:
  - Cheap
  - Effective
  - Easy to pull off
- Phishing through e-mail marketing services
- Thefts of school district funds last year, ranging from a low of $206,000 to a high of $9.8 million

Breaches Impacting School Vendors and Other Third Parties

- Service providers often access, process, or host sensitive or confidential organized data, including employees' and customers personal information
- Organizations also rely on vendors to provide business critical operations and services, such as interacting with customers or managing IT systems.
- Proper vendor management for privacy and data security issues ensures that:
  - Vendors deliver their services in compliance with the organization's privacy and data security requirements
  - The organization complies with its own regulatory and legal obligations regarding privacy and data security
- Pre-engagement due diligence
- Establish a vendor management process

Class Invasions, DoS Attacks and Related Disruptions

- Class/meeting invasion is defined as incidents where unauthorized individuals disrupt online classes
- Impacts on schools and their communities, including:
  - Class disruptions and cancellations, and—in more extreme circumstances—school closures
  - School board meeting disruptions and cancellations
  - Disruption of email service to and from school community members
  - The exposure of young children and youth to racist, sexist, and anti-Semitic hate speech; threats of violence; live sex acts; and pornography
- DoS (**D**enial **of** **S**ervice) and DDoS (**D**istributed **D**enial **of** **S**ervice) attacks flood internet-available websites, computers, or other resources with excessive network traffic in an attempt to deny access or services to legitimate users

Threat Actors Exploit False Sense of Security in the Cloud

- Cloud environments are continually being put to the test during this challenging time
- Cloud computing services take many forms and generally offer online access to shared computing resources with varying levels of functionality depending on the users' needs, such as:
  - Data storage to complete software solutions
  - Platforms to help application developers create new products
  - Full computing infrastructures to deploy and test programs
- Cloud services often include on-demand internet access to computing services
- Greater cybersecurity risks resulting from cloud computing
- Hasty deployment of cloud-based collaboration services may result in oversights in security configurations

What to Expect

- **Nation-state sponsored actors**:
  - Attacks against human rights and democratic systems
  - Disinformation campaigns
  - Uncontrolled cyber-arms race
  - Data theft
- **Cyber-offenders**:
  - Sextortion
  - Cyberbullying
- **Cyber-criminals**:
  - Deep fake
  - BPC (**B**usiness **P**rocess **C**ompromise)
  - BEC (**B**usiness **E**mail **C**ompromise)
  - Malware