Cybersecurity Incident Types

Did You Know?*

27.9% likelihood of a recurring material breach over the next two years

28% of all cyber attacks in 2018 involved insiders

43% of all cyber attacks are aimed at small businesses

$59 Billion – cost of malicious activity to the U.S. Economy

197 day mean time to identify a breach

17% of breaches were attributed to human error

What are the effects of Cyber Incidents on Small Businesses?

- ***Slows down devices and productivity***
- ***Recovery is resource intensive***
- ***Data losses and lockouts affect customers***
- **System performance or availability is compromised, stifling potential revenue**
- **Potential additional surge fees to internet service providers.**

Malware

What is it?
Malware or "Malicious Software" is an term that describes any harmful malicious program or code. They seek to invade, damage, or disable electronic devices by taking partial control via the use of trojans, ransomware, crypto-miners, keyloggers and worms

Preventative Measures
- Back up your data
- Keep software up-to-date
- Restrict access to third party vendors

Unauthorized Access

What is it?
When an unapproved entity that gains access to a website, database, system, server or system violation of the organization stated security policy. This includes external, and internal threats as well as third party breaches

Preventative Measures
- Strong security policy and controls
- Third party security compliance
- Employee monitoring

Data Breaches

What is it?
An unauthorized viewing, stealing or use of a sensitive or confidential data. Data breaches may affect personal heath record, personal identifiable information, trade secrete or intellectual property

Preventative Measures
- Security awareness training
- Encrypt data
- Vulnerability assessment
- Regular database and network patching
- Employee monitoring

**** To learn more - see attached sheet of reference citations***

Distributed Denial of Service(DDoS)

What is it?
The fundamental premise of DDoS attacks is to flood an organization's websites with so much network traffic they can't function properly. Often DDoS is used to hide more serious attacks of another type

Preventative Measures
- Apply all relevant security patches, periodic testing
- Shut down unnecessary services/ports
- Protect against *botnets*: expert detection of unusual and excessive traffic, deflection and quarantine

Social Engineering

What is it?
The act of manipulating people into willingly divulging or granting access to data. Common sub-types include phishing, baiting, and tailgating

Preventative Measures
- Be wary of unsolicited e-mail, text, and phone calls
- Do not respond to requests for personal information from unknown sources
- Apply e-mail filters or spam-tagging to reduce traffic
- Test employees. Engage an IT service to send spoof phishing e-mails

THE NATIONAL CYBERSECURITY SOCIETY

Cyber Incident Response Framework

Investigate → **Identify** → **Contain** → **Eradicate** → **Lessons Learned**

Cyber Incidents Infographic References:

The best protection is awareness and education source:
https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing#spear-phishing

Social Engineering Sources
https://www.us-cert.gov/ncas/tips/ST04-014
https://www.wsj.com/articles/see-how-much-you-really-know-about-cybersecurity-11559672037?mod=searchresults&page=1&pos=3
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/phishing
https://apwg.org/reportphishing/ https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing#spear-phishing
https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/phishing#spear-phishing

$59 Billion cost source:
https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf?mod=article_inline
43% cyber attacks source
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

DDoS Sources:
https://enterprise.verizon.com/resources/reports/dbir/
https://www.alienvault.com/blogs/security-essentials/distributed-denial-of-service-attacks-protection-methods-and-best-practices

Unauthorized Access:
https://medium.com/mimir-blockchain/4-cybersecurity-facts-every-business-should-know-f59a4a56e12e
https://huntsource.io/preventing-responding-third-party-security-breaches/
https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view