DS24
DataSure Twenty Four
Your Cybersecurity Partner

DataSure24's November Brainbytes: Incident Response Plans

DataSure24 is your cybersecurity partner, working to help meet your company's specific security needs. Each month, we'll offer bytes of information about emerging risks, news, and protective measures to help keep your data safe and your network secure.

Malware. Phishing. DDoS. Insider Threat. Zero-Day Exploit. The number of cybersecurity attack incidents continues to increase exponentially:

- Cyber-crimes are expected to cost the world $10.5 trillion USD by 2025.
- Small to medium-sized businesses are three times more likely to be attacked by cyber-criminals as compared to large businesses and corporations.
- During the third quarter of 2022, internet users worldwide saw approximately 15 million data breaches, up by 167% compared to the previous quarter.
- 241,206 incidents reported to law enforcement and banking institutions between June 2016 and December 2021 totaled domestic and international losses of $43.31 billion.
- Ransomware and destructive attacks represented 28% of breaches amongst critical infrastructure organizations, in efforts to disrupt global supply chains.

Even cases involving the same type of cyberattack can vary in scope and overall impact. The few constants in cyberattacks include disruption and loss, of: information, revenue, productivity, reputation, safety and trust.

Ransomware, for example, is a type of malicious software (malware), that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.

These attacks have the potential to bring business operations to a complete halt, a devastating impact on a business. The business leader of a U.S.-based manufacturing company equated it to being “punched in the stomach and losing all the air in your diaphragm, and about four weeks later, learning how to breath again."

During the first half of 2022 alone, 236.1 million ransomware attacks were reported world-wide. In addition, there have been 2.8 billion malware attacks so far this year, up by 11% when compared to 2021.

- **Manufacturing experienced more attacks than any other industry** (23%) in 2021. 47% of these attacks were due to vulnerabilities in cybersecurity.
- **U.S. financial institutions reported more than $1 billion in potential ransomware-related payments** in 2021 — almost triple the amount from 2020 and the most ever reported.
- The number of healthcare breaches in the first half of 2022 was nearly double that of the same period in 2021. **The per-incident cost of a healthcare data breach: $10.1 million**
- Ransomware attacks at school districts are not at all unprecedented: Hundreds of K–12 **school districts have publicly disclosed 1,300 cyberattacks**, including ransomware attacks, since 2016.

The stats go on and on. So what should businesses do?

How to Respond to a Ransomware Attack:

1. Do Nothing
2. Pay the Ransom

How to REALLY Respond to a Ransomware (or ANY Cybersecurity Attack):

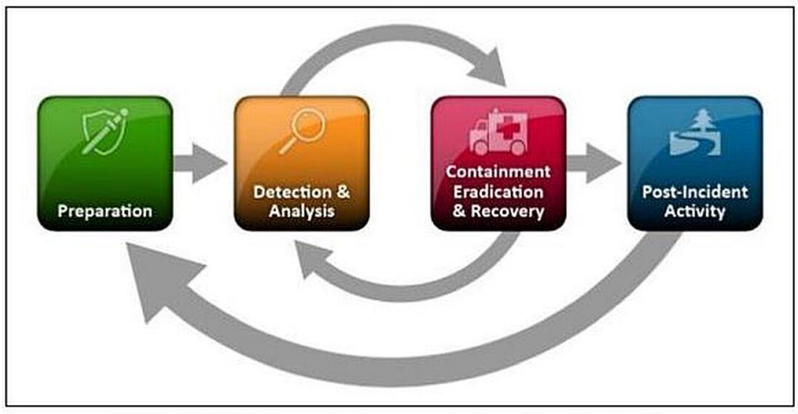
1. *(Insert Your Company's Incident Response Plan Here)*

An Incident Response Plan is vital to combat not only ransomware attacks, but any and all cybersecurity attacks.

A company's Incident Response Plan:

- Outlines how to minimize the duration and damage of security incidents
- IDs Stakeholders
- Streamlines Digital Forensics
- Improves Recovery Time
- Reduces Negative Publicity
- Reduces Customer Turnover

Four Components of an Incident Response Plan



NIST SP 800-61 *Computer Security Incident Handling Guide*

An Incident Response Plan should address ALL possible scenarios in response to a successful cyberattack. For example:

- What data and/or systems are affected?
- Who is the first person to call?
- How do I communicate?
- How can I access my data?
- Is there a back-up system that's not connected to the internet?
- How do I run the business, keep operations going?
- What information do I need to keep a hard copy of in my file cabinet?

While it's impossible to remove all security issues, an **effective Incident Response Plan can mitigate the largest cybersecurity threats.**

Cybersecurity should always be a business priority. ***Unprepared organizations will become easy targets for cyberattacks.*** *Now is the time to learn the potential cybersecurity risks for your business, and build a complete cybersecurity plan.*

For more info on making a plan, check out our latest blog: Incident Response Plans: A Tool in Your Arsenal Against Cyberattacks

If you would like to speak more about how DataSure24 might help your company meet its security needs, contact us by clicking below, or call (716) 600-3724. We look forward to hearing from you!

Email Us!
