TREXIN INSIGHT PAPER

December 14, 2022

CYBERATTACKS

Recovering from a breach.

Cybersecurity breaches have become increasingly common in recent years: according to Identity Theft Resource Center (ITRC), data breaches increased 14% in the first quarter of 2022.

The global COVID-19 pandemic jumpstarted a 'work from home' movement. This shift has created a mobile, distributed workforce, which has emboldened cyber criminals by providing multiple entryways into an organization. Due to this increased interconnectivity, cyber criminals have multiple lower risk opportunities to infiltrate an organization's environment and commit fraud. Phishing attacks, for example, remain a common and effective method for cyber criminals to get access to personal and financial data. With a spike in the number of attacks and increasing sophistication of cyberattacks, businesses should revisit (or develop for the first time) their plans for detection, mitigation, and returning to business as usual.

Upcity Reports states that only 50% of U.S. businesses have a cybersecurity plan in place; of those, 32% have not changed their cybersecurity plan since the pandemic forced remote and hybrid operations. As the threats evolve, cybersecurity must evolve as well. Cybercrime cost U.S. businesses more than $6.9 billion in 2021. IBM's Data Breach Report shows that the average cost of a data breach in 2021 rose to $4.24 million per incident, the highest in the history of the report.

At this point it's not a question of "if" a company will be a victim of a cyberattack, it's a question of "when". Even with the best technology and IT policies, your organization likely will become a victim of a cyberattack. With ever-changing technology to fight cyberattacks, companies are focusing on implementing newer security techniques to keep their data and environment safe. There are steps that your organization can take which will help ensure that your organization and customers suffer minimal damages after a breach.

1. **Incident Response Plan (IRP)**

   An IRP is a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattacks. An IRP provides structure and guidance in a high-stress situation. If you do not already have an IRP document, and identified your Incident Response Team, identify that team and make/implement an ad-hoc emergency response plan as soon as possible. You should focus on organizational responsibilities and communications. It is particularly important that everyone involved knows their tasks and no miscommunication occurs. If incorrect information gets leaked, it can lead to further damages to the organization and the brand image. Therefore, it is of utmost importance that an IRP is in place. Having an ad-hoc one is better than not having one. An IRP will assist in limiting the impact and helping your business to recover faster.

2. **Prevent Escalation / Isolate Network(s)**

   Determine the scope of the attack by identifying which business unit, department, or specific database has been impacted. Assess the damage and isolate the affected network(s). Network segmentation will assist to minimize the impact on other assets and provide additional security and control. You can reroute, filter, or block traffic on the affected networks.

3. **Assess the Vulnerability**

   A deep analysis will help uncover the attacker and lapses in the company's security. Develop a plan to systematically review the weakness in the environment. There are several types of assessments you can do such as Network, Database, and Applications. Vulnerabilities that are recorded can be assigned levels. You can then leverage internal or hired Subject Matter Exerts to give recommendations for remediation, and mitigation plans can be made accordingly. Assessing and identifying your organization's vulnerabilities brings you one step closer to a safer and more secure environment.

4. **Close the Vulnerability**

   Deploy cybersecurity controls and policies to prevent similar attacks from happening in the future. An in-depth postmortem after such situations often leads to uncovering the lapses in cybersecurity and business controls. In addition to this, make sure you have an IRP in place (if you did not have one prior to the attack). Having a process in place to recover from a breach makes it easier to return to normal business operations.

5. **Record the Details**

   As you move through the steps, make sure everything—the what, when, where, how, and which areas were impacted—is documented. Also include details of the steps taken to secure the business, counter the attack, and return to normal business operations.

   It is necessary to integrate cybersecurity into your business plan. Security policies and an IRP assist in making it through a cyberattack. Having a team assigned, and responsibilities laid out, makes things go much more smoothly. Organizations need to assess their process and procedures and continually improve them.

Click here to learn about Trexin's Cybersecurity Practice Area and how we can help you with the steps listed above.

REFERENCES

https://betanews.com/2021/12/20/cybercriminals-penetrate-93-percent-of-company-networks/
https://upcity.com/experts/small-business-cybersecurity-survey/
https://www.ibm.com/reports/data-breach
https://www.embroker.com/blog/how-to-recover-from-a-cyber-attack/
https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf
https://csrc.nist.gov/glossary/term/incident_response_plan#:~:text=Definition(s)%3A,organization's%20information%20systems(s)

This TIP was written by Fatima Zehra. Fatima welcomes comments and discussion on this topic and can be reached at fatima.zehra@trexin.com.