COMPASS
CYBER SECURITY

CYBERSECURTIY INCIDENT RESPONSE

No organization is exempt from cybersecurity threats in today's digital environment, as they affect businesses of all industries and sizes. As a result, having an established incident response plan is critical to minimizing the cost of a breach, reducing the data loss, and maintaining the organization's reputation.

When a cyber security incident is discovered, it is crucial to act quickly and effectively to limit the breadth of the attack. Below are the first steps your organization should take if you experience a breach:

1. **CONTAIN, DEFINE, AND DETECT:** Identify what part of the network was compromised and isolate it immediately. Determine what type of incident occurred and respond accordingly.

2. **DOCUMENT THE BREACH:** Record the date and time the breach is discovered and the devices/data that have been compromised.

3. **COMMUNICATE TO KEY STAKEHOLDERS/EMPLOYEES:** As soon as an attack is identified, mobilize your team of employees across all facets of the business and put your incident response plan into action.

4. **RECOVER INFORMATION AND BACKUPS:** Switch to backup servers to restore any information that was saved prior to the breach.

5. **GATHER FORENSICS FROM THE AFFECTED SYSTEMS:** Get an idea of what occurred on the server at the time of the event. This should include personnel working on the affected system, network topology diagrams, recent system additions and relevant communications.

6. **NOTIFY AUTHORITIES AND AFFECTED PARTIES:** Be familiar with your state's data breach notification laws and begin to inform those who may have had their information compromised. Failure to notify potential victims could result in legal action.

7. **INITIATE MEASURES TO PREVENT FUTURE ATTACKS:** Conduct post-incident reviews with all relevant personnel. Consult outside resources to mitigate your vulnerabilities so another breach does not occur. Continue to monitor the affected systems as the attacker may have installed a "back door" you missed.

WHAT NOT TO DO IN THE EVENT OF A CYBER SECURITY INCIDENT

- Do not turn off servers in an attempt to stop the attack.
- Refrain from using the affected systems to communicate about the incident.
- Do not attempt to hack into the cyber criminal's attacking system. This is illegal and could result in criminal penalties.

THERE ARE MORE THAN 2,600 RECORDS STOLEN EVERY MINUTE.

For more information, please contact
info@compasscyber.com or 667-401-5108.

COMPASSCYBER.COM