PREPARING FOR A CYBER INCIDENT AND DATA BREACH

Being proactive is an important step in preventing or reducing the risks of a cyberattack. Conducting a privacy and security assessment before an incident will help you reduce your risk of a data breach. The following are steps organizations of all sizes should consider taking:

Invest in technical data security controls and procedures to deter or prevent cyberattacks. These security measures can include:

- Dual authentication
- Adequate firewalls and secure configurations
- Strong passwords, changed frequently, and adequately protected
- Encrypting important or sensitive data and personal information
- Using current anti-virus software and other measures to protect against malware
- Performing network scans to assess vulnerabilities
- Deleting of sensitive information when it is no longer needed

Adopt an incident response plan and reporting mechanisms so management is promptly advised of all cyberattack incidents.

Not only should all employees be trained on the possibility of cyberattacks and where attackers are most likely to direct them within the company, but the incident response plan should be tested regularly.

Know where data is stored.

Knowing where a company's data is stored will aid in making decisions about how to best protect data, evaluate compliance with applicable data security laws, and respond more efficiently and effectively if an incident occurs.

Implement a data retention policy.

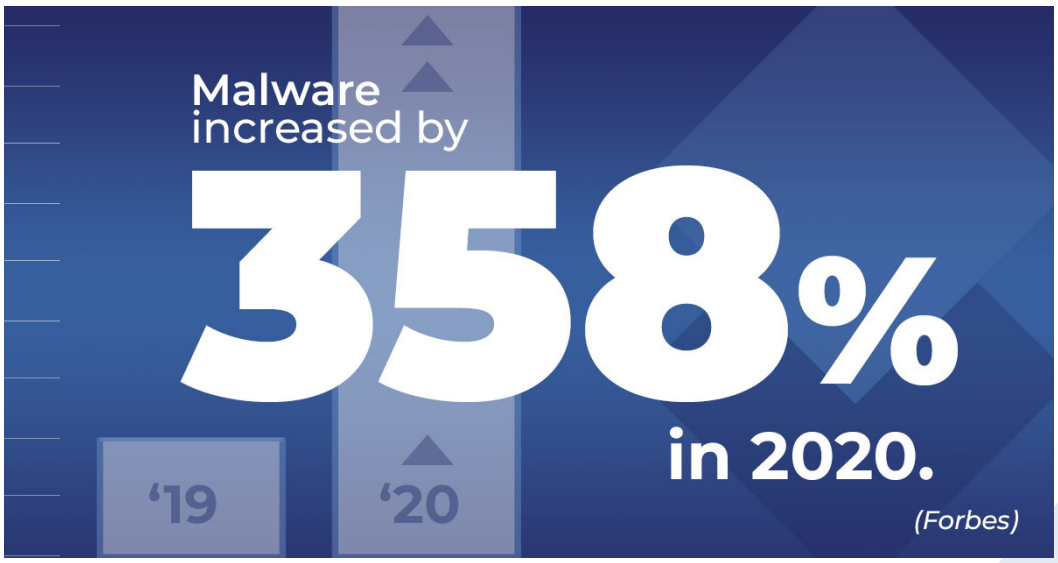
Retain only the data the company needs for business operations and only for the legally required period of time.

(continued on next page)

PREPARING FOR A CYBER INCIDENT AND DATA BREACH *(continued)*

Review contracts with vendors/business partners.

A vendor's network could be used as a launching pad for an attack. Review contracts with vendors and other business partners to ensure they appropriately address responsibility and liability for data security and provide for regular audits to ensure compliance.



Develop a work plan—employee training.

Physical safety measures are just as important as technical safety measures. Implement a written compliance program applicable to the company's processes and people. Train, and retrain, employees on a regular basis to recognize potential data privacy and cybersecurity vulnerabilities.

Obtain insurance coverage and mitigation.

Consider obtaining cyber liability insurance. No security measures are perfect and the costs of a breach can be catastrophic. When selecting a policy, consider whether it includes coverage for response, remediation, and litigation costs.

A BREACH HAS OCCURRED – CYBER INCIDENT RESPONSE PLAN

Your company has experienced a cyberattack and there has been a data breach. The following are critical components of effective incident response:

Mobilization of necessary personnel

- Legal
- Information Technology Department
- Management
- Investigate – Forensics
- Public Relations

Containment and analysis

- Secure network
- Determine scope
- Establish accountability
- Implement incident response plan
- Identify source of the attack
- Preserve evidence
- Remediate and recover

Communications and notification

- Evaluate breach notification obligations
- Evaluate coordination with law enforcement/regulators
- Consider potential public relations issues
- Prepare and distribute notifications

Moving forward

- Post-incident review
- Remediate security gaps
- Provide additional training
- Improvements to response policies and procedures

Ruder Ware 100 SINCE 1920

BUSINESS ATTORNEYS FOR BUSINESS SUCCESS®

wausau | eau claire | green bay ruderware.com

visit our blogs at *blueinklaw.com*