How to Avoid a Major Security Incident, and What to Do if One Occurs.

LeapFrog®

How to Avoid a Major Security Incident, and What to Do if One Occurs.

Every day, your business faces countless security risks, with nearly 4,000 cyber threats and attacks occurring globally. A ransomware attack strikes a company every 14 seconds, leading to potentially devastating financial consequences. From phishing emails to brute force attacks, any suspicious activity can be considered a security event. Once sensitive data is compromised, the situation escalates to a full-blown security incident. Small businesses are even more vulnerable, since they typically lack resources to implement strong cybersecurity measures. Being aware of these threats and having a robust incident response plan is crucial to safeguarding your business.

How do I minimize the amount of security events?

There are several ways to implement security measures for your business:

Assess Your Current Cybersecurity Posture

- **Evaluate Existing Security Measures:** Review your current cybersecurity practices, including firewalls, antivirus software, and data encryption.
- **Identify Vulnerabilities:** Conduct a risk assessment to identify potential weaknesses in your IT infrastructure and processes.
- **Understand Compliance Requirements:** Determine any industry-specific regulations or compliance requirements that apply to your business.

Implement Preventative Measures

- **Firewalls and Network Security:** Install and maintain firewalls to protect your network from unauthorized access. Use intrusion detection systems (IDS) to monitor for suspicious activity.
- **Data Encryption:** Encrypt sensitive data – both at rest and in transit – to protect it from unauthorized access.
- **Access Controls:** Implement strong authentication mechanisms, such as multi-factor authentication (MFA), and enforce least privilege access policies.
- **Employee Training:** Provide regular cybersecurity training to employees to help them recognize and avoid phishing attacks and other social engineering threats.

Establish Detective Measures

- **Monitoring and Logging:** Use security information and event management (SIEM) systems to monitor network traffic and log activities for potential threats.
- **Regular Security Audits:** Conduct regular security audits and vulnerability assessments to identify and address potential security gaps.
- **Incident Response Plan:** Develop and document an incident response plan to quickly address and manage security incidents when they occur.

Define Corrective Measures

- **Incident Response Procedures:** Establish clear procedures for responding to security breaches, including containment, eradication, and recovery processes.
- **Data Backup and Recovery:** Implement regular data backups and ensure that you have a robust disaster recovery plan in place to restore systems and data after an incident.
- **Continuous Improvement:** Regularly review and update your cybersecurity policies and procedures based on lessons learned from security incidents and evolving threats.

Engage with Cybersecurity Experts

- **Consult with Experts:** Engage with cybersecurity consultants or managed security service providers (MSSPs) like Leapfrog to gain additional expertise in implementing and maintaining your strategy.
- **Stay Informed:** Keep up to date with the latest cybersecurity trends, threats, and best practices to ensure your strategy remains effective.

Communicate and Document

- **Document Your Strategy:** Clearly document your cybersecurity policies, procedures, and incident response plans.
- **Communicate with Stakeholders:** Ensure that all stakeholders, including employees and partners, are aware of and understand your cybersecurity practices and policies.

How do I know if my company's data has been compromised?

Other than the obvious signs of a complete system crash or alerts from your protection methods, many data breaches may be subtle. Watch for unusual traffic volumes or suspicious activity across your infrastructure. Mixed-up data or the addition of unrecognized software can also be an indicator an event has occurred.

A dark web monitoring service will continually monitor the dark net market and other data stores for your information and alert when it is found. Alerts would be sent to you on what has been discovered and recommendations on actions to be taken to protect yourself before the information is leaked, sold, or used to compromise your organization.

What should be done if a security incident has occurred?

Quick responses to incidents are key in minimizing fiscal damages and protecting a company's reputation. Once a threat has been noticed, avoid panic and communicate effectively with your team. Having a plan ready to implement before a compromise is critical to being able to act with speed and have an effective outcome. Containing the incident, securing the network, and preserving log data should be the top priority.

Remember – cybersecurity is a continuously evolving method of protection. Your strategy must consistently be updated to address new types of threats, your technology should always be up-to-date, and your entire IT infrastructure needs to be monitored for vulnerabilities.

Having a plan in place BEFORE an event could potentially save your business. Knowing who to contact and what to have prepared for law enforcement, insurance, and technology providers will help each of these organizations move quickly, saving valuable time and money.

Consider partnering with a third-party provider that offers IT and Cybersecurity services, such as Leapfrog, to ensure your IT operates seamlessly and securely. Read more about the benefits of Outsourced IT Services for Small to Medium-Sized Businesses (leapfrogservices.com).

Leapfrog offers peace of mind by protecting, monitoring, and defending your IT infrastructure. Their team of trained professionals consistently performs surveillance on your IT environment. If a security incident occurs, multiple teams respond to work alongside your CSO and internal team. To learn more, leap over for a conversation.

Contact us today at: 866.260.9478 to talk with our experts.

Leapfrog offers outsourced managed IT and cybersecurity services that fit easily into your business model. With over 25 years of MSP, MSSP, and CyberRisk Management experience, we help a broad array of companies simplify their IT operations while improving their security and resiliency. Our services are scalable, aligned, and built on a proven methodology, and our culture (we call it "Frogma") is built on Integrity, Service, and People so you get personalized, best-in-class support.

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

If you're ready to take your IT and cybersecurity services to the next level, Leapfrog is ready to help. Please call 866-260-9478 or contact us at sales@leapfrogservices.com.