groupsense

PROTECT YOUR ORGANIZATION FROM CYBER INCIDENTS

What Threats Does Your Organization Face?

According to Accenture's Cost of Cybercrime Study, 43% of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves.

Business Email Compromise (BEC) is a form of attack where an outsider gains visibility to email systems to carry out a financial crime. The attacks vary in nature, but most often, the intruder will monitor communications for some period of time, gaining an understanding of the organization, customers, and suppliers. Eventually, they will send fraudulent emails asking staff to wire money or change routing numbers for payments resulting in payments to the attacker's accounts rather than the intended recipient. These attacks are statistically causing more financial harm than ransomware nationwide.

Ransomware is a form of cyber attack where the attackers gain access to company systems. To carry out the attack, they steal company data and use software to encrypt the company systems. In most cases, the only way the systems can be unlocked is to pay the ransomware perpetrators. This is most often done via cryptocurrency like BitCoin. These attacks are highly disruptive and opportunistic. The key to preventing ransomware attacks is employing some basic cyber hygiene practices.

An FBI study that examined 241,206 BEC incidents found that the combined domestic and international losses incurred amounted to US $43.31 billion between June 2016 and December 2021.

Protecting Your Organization

Both ransomware and BEC attacks are commonly caused by preventable security gaps. By promoting and participating in the following activities and behaviors, your organization can reduce its cybersecurity risk.

Business Planning

Email & Email Policy

Have a strong policy about using a corporate email account for personal use. Restrict access to personal mail on company assets to further reduce your organization's risk. Barr the use of corporate email credentials to create accounts on anything unrelated to the business without permission.

Security Awareness Training

Education solves nearly everything. Your staff will always be the weakest point in your security program. In order to combat threats, the team needs to be made aware of them and taught how to identify and avoid pitfalls that bypass your security efforts.

Password Policy

Maintain and publish a password policy for your organization. The policy should illustrate the importance of password security and credential use in the organization. One of the most common points of entry for an attacker is credential reuse or stuffing, where threat actors leverage breach data or stolen credentials from a third party. This happens when corporate staff uses their corporate email for a third-party, non-business-related (or business-related) site and that site gets compromised. Matters are made worse when employees use the same or similar passwords that they use for corporate access. To prevent this, your organization can use a credential monitoring service (also referred to as Account Takeover Protection, ATO) to determine if/when your staff does this and is affected by a third-party breach, reset their password internally if affected, and send them an official notification of policy violation.

Approval Processes

Require a multi-step approval process for any modification to financial records and payments. For example, no changes should be made to payee account information without a phone call to the payee via a contact number on record. Further, no wire transfers or sudden large purchases should be made unless two or more of the executive team are contacted via phone and send written approval.

Business Planning

Insurance

Consider a cyber insurance policy. There are providers that offer affordable solutions to businesses.

Employee Resource Access

When a staff member leaves the company, regardless of the reason, have a process in place to remove their access to business systems and communicate the departure to staff and partners.

Continuity Plans

Develop and practice a response plan. The plan should contain at a minimum:

- Contact information for IT and incident support during an attack
- A list of roles and responsibilities during the incident
- A business impact assessment and plan to restore/continue operations
- A list of the tools and methods available for analysis and recovery
- Internal, external, and affected party (clients for example) communication plan

Technical Tips

Patch Your Systems

When software vendors make mistakes that sometimes lead to cyber risk, they offer updates to fix those mistakes. It is common to ignore these warnings, but resisting the urge to do this and updating your systems as often and as quickly as possible goes a long way in preventing cyber attacks.

Enable MFA Wherever Possible

Enable the two-factor authentication (2FA) or multi-factor authentication (MFA) capability on everything used in the business, including email, network access, remote access, and any web-based applications.

Use a Password Manager

Use a password manager and require employees to use this as part of the organization's password policy. Most password manager programs offer a corporate license which allows you to provision and de-provision users centrally. They also allow you to manage policy around the frequency of password-forced resets and password complexity.

Secure Remote Access

If remote access is required, use a zero-trust access method or a VPN in conjunction with two-factor (2FA) authentication. Avoid remote desktop (RDP) or direct-to-machine access whenever possible.

Technical Tips

Anti-Phishing

Phishing is when a bad actor sends an email to your staff with a link that will install malicious software or similar on their computer. These are carefully crafted and often hard to detect. There are numerous software and SaaS/ anti-phishing solutions that will protect your staff from clicking on malicious links.

Monitor for Lost Data

Most cyber incidents are predicated on the attacker having access to data about your organization they should not have. Employ a Digital Risk monitoring solution to look for that data and help clean it up. These solutions also give visibility to policy violations, like the credential use policy.

Backups

Keep at least one manual backup of your data offsite in a secure location. Many disaster recovery plans only account for a hot backup, taken when users are online, and a warm backup, taken when servers are running but not in use. It is best to also use an auxiliary backup solution beyond what your cloud storage provider offers. There are many solutions that integrate seamlessly with Google, Azure, and other cloud providers. Finally, CHECK to make sure the backup solution is functioning properly on a regular cadence.

Encrypt All Devices and Storage

Utilize host-based encryption where possible to encrypt data at rest. This is available natively on most operating systems.

About GroupSense

GroupSense is a digital risk protection services company that delivers customer-specific intelligence that dramatically improves enterprise cybersecurity and fraud-management operations. Unlike generic cyber-intelligence vendors, GroupSense uses a combination of automated and human reconnaissance to create finished intelligence that maps to each customer's specific digital business footprint and risk profile. This enables customers to immediately use GroupSense's intelligence to reduce enterprise risk, without requiring any additional processing or management by overstretched security and fraud-prevention teams. GroupSense is based in Arlington, Va., with a growing customer base that includes large enterprises, state and municipal governments, law enforcement agencies and more.

Want to understand your organization's risk profile?

Schedule a complimentary briefing with GroupSense experts today or visit the website, www.groupsense.io, to learn more about Digital Risk Protection.

Schedule a Briefing