groupsense

PRIORITIZING CYBERSECURITY: TIPS TO BETTER PROTECT YOUR DATA

GroupSense does some of the largest negotiations for ransomware. Ransomware is a quick and easy path to revenue for criminals. Unfortunately, ransomware isn't always the first play in a criminal's playbook. They usually have been in your network for a while and deploy ransomware after they've accessed all your data. GroupSense's team of experienced negotiators developed cybersecurity tips to help reduce your risk.

PATCH YOUR SYSTEM

Just do it.

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 re-use or stuffing, often leveraging breach data or stolen credentials from a third-party. This happens when corporate staff use their corporate email for a third party non-business related (or business related) site and that site gets compromised. Matters are made worse when they use the same or similar passwords that they use for corporate access. Use a credential monitoring service (also referred to as Account Takeover Protection, ATO) to determine if/when your staff does this and are affected by one of these third-party breaches. Then reset their password internally and send them an official notification of policy violation.

USE A PASSWORD MANAGER

Use an enterprise-friendly password manager and require employees to use this as part of the security program. Most password manager programs offer a corporate license which allows you to provision and deprovision users centrally. They also allow you to manage policy around the frequency of password forced resets and password complexity.

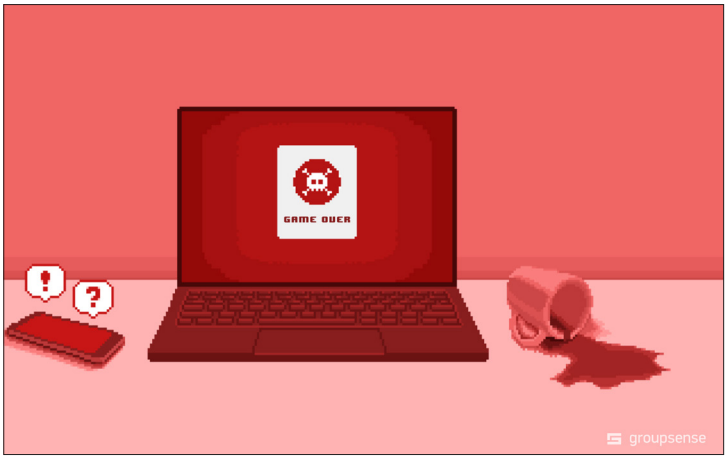
ENABLE MULTI-FACTOR AUTHENTICATION EVERYWHERE POSSIBLE

Enable the 2FA or MFA capability on everything used in the business. This includes email, network access, remote access, and any web-based applications. You may or *should* choose to evaluate SaaS vendors based on their ability to offer this as protection. Favor solutions that offer MFA through a mobile application or hardware token over SMS only.

Prioritizing Cybersecurity: Tips to Better Protect Your Data

EMAIL, EMAIL POLICY, ANTI-PHISHING

Have a strong policy about using corporate email for personal use. Restrict access to personal mail on company assets. This reduces your phishing attack surface tremendously. There are numerous SaaS / Cloud based anti-phishing solutions that will protect your staff from clicking on bad things.



SECURE REMOTE ACCESS

If remote access is required, use a zero-trust access method or a VPN. Use two-factor authentication. Always. Avoid RDP or direct to machine access whenever possible.

BACKUPS

Keep at least one manual backup of your data offsite in a secure location. Many disaster recovery plans only account for a hot and warm backup. Also, it is best to use an auxiliary backup solution beyond what your cloud storage provider offers. There are many solutions that integrate seamlessly with Google, Azure, etc. Finally, CHECK to make sure the backup solution is functioning properly on a regular cadence.

Avoid full backups on the weekends. It's a popular decision for organizations to conduct a full backup on the weekend because there are fewer users that could be disrupted. However, it's also the choice time for threat actors to run their ransomware. For starters, they know there are fewer users on the network and their ransomware has a lower chance to be detected, which means a higher disruption chance for you and a higher success rate for the attackers. Secondly, the TAs know the ransomware might interfere with your full backups which creates more leverage for them during a negotiation.

INSURANCE

Consider a cyber insurance policy. There are smaller providers like Cysurance that can be affordable to small businesses.

ENCRYPT ALL DEVICES AND STORAGE

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

THREAT INTELLIGENCE / DIGITAL RISK PROTECTION

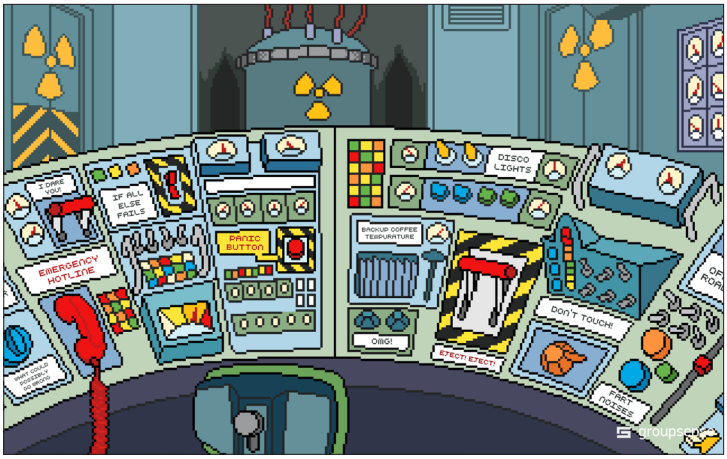
The indicators of compromise (IOCs) related to malware strains associated with ransomware are quickly and easily available on the internet. A solution providing Digital Risk Protection will monitor open source repositories, code repositories, cloud storage buckets, paste sites, the dark web, and social media for:

- Data Leaks
- Intellectual Property Leaks
- Stolen System Access
- Fraudulent Domains (look-alikes)
- Stolen or Leaked Credentials
- Planned Attacks
- Brand Fraud
- Fraudulent Mobile Apps
- And more...

Prioritizing Cybersecurity: Tips to Better Protect Your Data

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.



REGARDING REMOTE EMPLOYEES AND CONTRACTORS

If you are issuing devices to remote staff, install anti-virus and EDR software on the device. Consider also Managed Detection and Response (MDR) services, which will help monitor and manage the threats to those devices. For contractors, consider using VPS services and require those services to be used when interacting with corporate files, assets, code, etc. This mitigates the concern that they might steal those digital assets, or have an otherwise company issued machine stolen with the assets on it.

LOGS

Log everything and store centrally offsite. There are myriad services that will provide cloud log repositories. This becomes necessary when an incident occurs and you need to figure who took what, where, and when.

TESTING

Have some objective external tests done to your software and your systems at least bi-annually. You should have a human do these tests, though occasional automated vulnerability testing is also helpful.

PLANS AND SUCH

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

- Contact information for IR firm
- 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

Consider also retaining the IR firm in advance, as well as external counsel with breach experience, and PR.

EMPLOYEE RESOURCE ACCESS / DE-PROVISIONING

A quick note on onboarding and offboarding. Well, specifically offboarding. Do that. Have a process for removing employees from corporate systems, notifying remaining staff and relative customers, and partners.

IF YOU ARE AFFECTED BY RANSOMWARE OR EXTORTION

Do not visit the threat actor victim site.
Do not attempt to negotiate with the threat actor.
Do not shut down or reboot systems.

Do contact legal counsel with breach experience.
Do contact an experienced negotiator.
Do contact an incident response firm.

GroupSense's Ransomware Response Readiness Subscription (R^3S) gives organizations the best chance to survive and recover. Receive the intelligence you need to take action quickly and decisively. If you'd like to talk to an analyst, contact us at **1-877-469-7226**, or email **sales@groupsense.io**

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.

Find out how GroupSense can help your organization at www.groupsense.io