SeedPod CYBER

Risk Management for MSPs: Technical and Business Risk Reduction

In this short e-book, MSP executives can learn fundamental best practices for MSP risk management and come away with a 40,000-foot strategic plan that the IT or security team can run with and implement with executive direction and feedback.

It's clear to anyone that an MSP must evaluate risks, mitigate them, have plans for damage control, and mechanisms for continual evolution to new threats or changing environments. But where should you start, if a risk evaluation hasn't been done recently, or the plan in place is old, incomplete, or barely existent?

Start with the most obvious threats, in this ranked order

In creating and implementing a risk management plan, no MSP can do everything perfectly all the time, especially if embarking on a systematic plan for the first time. So, it makes sense to focus on the most common and biggest vulnerabilities first. Focusing first on the items in this list provide a solid foundation of risk management and hardening of your cyber defenses.

1. Backup loss and hardware failure

Just as most data breaches don't involve exotic hacks by highly intelligent criminals, not every data loss is due to a data *breach*. So, start with the basics. If your team doesn't have bulletproof safeguards to virtually eliminate risks related to **backup loss** and **hardware failure**, that's an easy, straightforward fix.

2. Phishing and stolen credentials

The 2022 Verizon Data Breach Investigations Report shows that phishing and stolen credentials remain in the top 5 sources of data breaches. It's another perennial reminder of a perennial challenge: if your team can get to data directly over the internet just by using login credentials, so can the criminals.

Theoretically, guarding against phishing and stolen credentials is a cheap, easy fix – just make sure your team members don't fall for phishing scams, use strong passwords, and safeguard their credentials. But that's only theoretical. In the real world, human beings need regular training on how to recognize phishing, and on how to follow strict best-practice protocols. And, it is important to follow-least provisioning of administrative credentials along with multi-factor authentication, to minimize threats due to credential take-over.

3. Ransomware

The same Verizon report indicates that an unfortunately upward-trending cause of data breaches is ransomware that spreads virally. The most common vectors, in order, include web apps, email, desktop sharing software, or simple carelessness in configuration.

This malware, once inside a system, can of course give bad actors the power to lock everything down and demand a payment that typically reaches into the millions of dollars – or less, for a smaller organization. Whatever the cost, the hackers calculate it to be doable, just barely worth the cost, and extremely painful.

The Verizon report classifies these breaches as Ransomware, because that's a very common use of them by the criminals – to enrich their coffers by demanding a ransom. But such viral malware can be used for other nefarious purposes such as stealing credit card data, identity theft, and taking control of vast numbers of computers for launching DOS attacks or mining bitcoin.

4. Manual Backdoors

These breaches occur when hackers probing web applications, or IOT portals through a system, etc., find ways to enter a system without using malware as described in the section above. The goals, and the results, are often the same, depending on the skill of the hackers and the vulnerabilities left open in the system.

Detecting such intrusions requires robust logging and analysis, so that software (and human agents) can detect threat *behavior*. The behavior of a bad actor differs dramatically from the legitimate uses of a system, for example massive downloading of files, to name just one. (Remember, a manual back door entry doesn't leave the "fingerprint" of a known virus, because there is no virus

at work. So, a strictly anti-virus defense would never detect a backdoor intruder.)

5. "Other"

The Verizon report has a disturbing entry in the top 5 most common actions resulting in data breaches. We've already covered the other four (see above). We've saved "Other" (which is actually 2nd-place in the data of the report) for last, because it's nebulous, containing a large number of disparate, sometimes highly technical breaching actions grouped together by necessity.

Defending against them is fortunately more straightforward than identifying each specific vector or action and plugging that hole. It's a matter of best practices. The rest of this article will summarize the foundation of a solid MSP risk mitigation and management strategy – guarding against not only the four easily-described threats above, but the longtail list of "other" possible breaches and losses.

Security controls MSPs should have in place

Endpoint Detection and Response (EDR)

The strongest, most comprehensive last-stand defense is EDR. EDR firms provide client companies with endpoint threat

detection services within their systems – not just perimeter defense, which is what traditional managed security service (MSSPs) or Managed Detection and Response (MDR) solutions provide. An EDR firm can also respond to threats once they are uncovered. It can perform these functions better and at dramatically lower cost than hiring and equipping an in-house team to detect and respond to threats.

Backups

Backups are fundamental to guarding against losses from breaches, as well as from incidents such as hardware failure or natural disasters. Common sense rules, and you should have adequate plans and follow the procedures religiously.

Logging & Alerting

Logging system behavior provides data for analysis in detecting threat behavior both real time and for forensic purposes. It enables security teams to better understand what is happening to quickly neutralize an attack or minimize damage as well as what happened, how it happened, and how to prevent it in the future.

Patching

MSPs should make sure that they use up to date versions of the software and apply all patches, whether from the core software, third-party software, or plugins. It's another defense which is "easy" in theory, but in the overstretched, rapid-paced real world

of business, IT teams, operations managers, and others need to follow up to ensure that the doors and windows are locked.

Role Based Access Control

Given that fact that MSPs have privileged access to their clients' environments, it is essential that that access be strictly governed. Role based access permissions should be based on least-use principles and general-use credentials should always be separate from privileged credentials.

Script Management

Scripts can be great tools to effectively and efficiently manage client's environments, but both the tools and the scripts themselves represent threats that can be used to compromise both the MSP and their clients.

Systems should be configured to deny scripts by default and to only whitelist those scripts which have been approved by management.

Multi Factor Authentication (MFA)

Perhaps the least expensive, most powerful defense against the most common breaches is multi factor authentication. MFA requires more than simple login credentials. Most Internet users are entirely familiar with it by now. After entering login credentials, for example, the system sends a one-time password to a user's phone. This exponentially decreases the likelihood

that an attacker can breach the system in the most common ways they do so – via phishing and stolen credentials.

Business risk reduction

Beyond the technical steps you can take to reduce risk, consider ways of reducing risk to your MSP business. Suppose you've erected and maintained the best technical and security training defenses possible. Hackers could still get through since no defense is 100% impenetrable.

How can you mitigate risk to your *business*, in the event of an incident?

Business is controlled by contracts, of course, so contracts are where you create firewalls to protect your business and the businesses of your partners and clients. Become aware of, and work to change if needed, contractual obligations concerning data breaches.

It's worth writing into your contracts, for example, obligations of clients to keep their systems up to date with security patches, to give just one concrete example.

Tech E&O / Cyber Insurance

Tech E&O and Cyber security insurance is another extremely valuable backstop to business losses in the event of a data breach. Since an MSP's largest potential E&O exposure is cyber related, purchase both the E&O and cyber insurance from the same carrier (which is usually offered on a combined form). That way you don't have to get in the middle of two carriers pointing fingers at each other when it comes to determining who is responsible for a claim.