datto

Information Security Analysis Program

2019 Case Study

In 2019, Datto sought a deeper understanding of the state of cybersecurity in the channel by learning firsthand from a group of managed service providers (MSPs) to surface their current internal practices. The program engaged with five United States-based MSPs across different size operations, traditional on-premises, and born-in-the-cloud footprints. Onsite engagements were one to two days at the MSP's location. Each engagement followed the methodology outlined in the following sections of this whitepaper, which has three pillars; a NIST Cybersecurity Framework (CSF) Benchmarking Exercise, Threat Modeling Exercise, and a Grey Box Penetration Test.

There was an expectation that the analysis conducted would show a correlation between the size of the MSP and the maturity of their security posture. As an MSP grows their related business risks also grow, and the thinking was that their security controls would mature alongside. After conducting the engagements, the findings surfaced something entirely different, showing that the size of an MSP does not necessarily correlate to an improved security posture.

This whitepaper is split into five sections:

- **Methodology -** A deep overview of the processes used by Datto to assess MSPs and their program. The intent here was to provide an outline that can be used by the community.
- **Key Trends -** Nine recurring themes surfaced during the case studies and are documented with additional context.
- **Recommendations -** A list of recommendations for posture improvement that all MSPs should review.
- **Notable Findings -** A comprehensive list of findings surfaced at one or more of the engagements.
- **We're Stronger, Together –** Wrap up of our findings and thoughts.

Methodology

When structuring the onsite engagements, Datto wanted to ensure they were free form enough to deal with the many unknowns but also recognized that consistency was necessary to measure the security posture across participants.

Discovery forms were sent ahead of each visit, outlining high-level details about the company, the client focus, business goals, and other attributes that were used in the analysis stage. Included in the discovery was a request for an Asset Inventory. An important note here, traditionally creating an Asset Inventory consists of naming every individual asset such as desktops, servers, switches, and printers that the MSP has within their network. Datto recognized that having that level of detail would not be necessary for this case study and opted for having summarized detail like the types of Operating Systems, Endpoints, and Datastores. Secondly, assets in the modern sense include cloud infrastructure, services, and other third parties, so for the remainder of this whitepaper, the Asset Inventory takes on this wider definition.

Key Trends
False Sense of Security
Basics Overlooked
Gaps Tend to Scale With Size
Tech Heavy and Process Light
Management of Vulnerabilities
Exposure to Security Practices
Detect, Respond, Recover?
Supplier Management
Incident Readiness

The final list of the requested information included IP address ranges, domains and URLs, desktop applications, and cloud services that individuals might use. These data points helped put the "grey" in the Grey Box Penetration Test for the engagement.

NIST Cybersecurity Framework

One of the three pillars of the engagement was the use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) for a benchmarking exercise. The NIST CSF was created to serve as a guideline for US-based private sector businesses to assess their ability to prevent, detect, and respond to cyber incidents. Version 1.1 of the framework contains 5 Functions, 23 Categories, and 108 Subcategories.

Initially, each Subcategory was scored using the Tier definitions set by NIST. However, this proved to be problematic and challenging to score in some situations. NIST created the Tier model to apply to the Categories themselves. Applying Tiers to the testing Subcategories leads to some undesirable outcomes. After some research, the engagements moved to an approach suggested by Jack Jones, a well-respected leader in information security and risk management, to measure Subcategories using a two-dimensional scale. For transparency, below are the definitions used how the rating system scored each Subcategory:

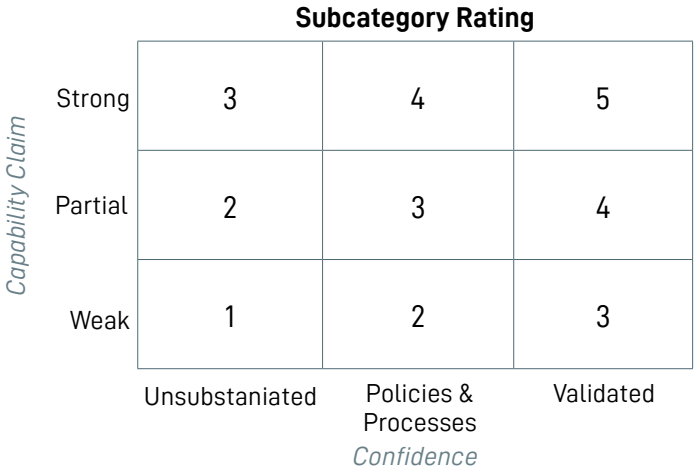

Figure 1

Capability Claim

- **Strong:** The Subcategory is both highly effective and has been implemented throughout most, if not all, of the organization
- **Partial:** The Subcategory is either highly effective but implemented across only a minority of the organization, or is in place throughout the organization but is marginal in its efficacy
- **Weak:** The Subcategory has either not been implemented at all, or is partially implemented and marginally effective

Confidence

- **Validated through Testing:** An independent party has evaluated the capability more than once, and at least once within the past year, and found it to align with the rating.
- **Substantiated by Policies and/or Processes:** The organization has formally defined expectations regarding the capability (usually thru policies and/or processes) that help to reduce the likelihood of the capability being ineffective or not meeting expectations.
- **Unsubstantiated:** There are no formal policies or processes that formally establish expectations for this capability, which increases the likelihood of it being ineffective.

The combination of Capability Claim and Confidence derived the final score for the Subcategory, as shown in **Figure 1.** The first two engagements were rescored using this approach, and the remaining engagements enjoy the ease by which this facilitated the conversation.

Conducting these served as the best means to understand and surface data used in the next pillar, the Threat Modeling Exercise. It's worth noting at this point, NIST CSF is risk-based, and in practice, a smaller MSP would not have the same level of risk as a large MSP. Having various levels of risk can translate into differences between companies who use NIST and is why Datto's use of the term benchmark is explicit here. While companies within the same peer group can share the scoring, a smaller MSP and a larger MSP should not compare themselves. Instead, a benchmark allows businesses to work through improvements to their program, and in 6 months to a year, step through the process to measure themselves again.

Threats

Before stepping through the Threat Modeling Exercise, it is worth discussing Threats, those targeting MSPs, and their clients. In more traditional terms, a Threat Actor is an individual or a group that is seeking to cause harm by leveraging a Vulnerability resulting in a system Compromise. For the remainder of this paper, Threats are simply the specific attack scenarios MSPs face against their environment.

Tactic	Technique	ATT&CK ID
Drive-by Compromise	Initial Access	T1189
Exploit Public-Facing Application	Initial Access	T1190
External Remote Services	Initial Access	T1133
Spearphishing Attachment	Initial Access	T1193
Spearphishing Link	Initial Access	T1192
Spearphishing via Service	Initial Access	T1194
Supply Chain Compromise	Initial Access	T1195
Valid Accounts	Initial Access, Persistence, Privilege Escalation	T1078
PowerShell	Execution	T1086
Third-party Software	Execution	T1072
User Execution	Execution	T1204
Brute Force	Credential Access	T1110
Credentials from Web Browsers	Credential Access	T1503
Credentials in Files	Credential Access	T1081
Application Deployment Software	Lateral Movement	T1017
Remote Access Tools	Command and Control	T1219
Standard Application Layer Protocol	Command and Control	T1071
Data Encrypted for Impact	Impact	T1486

The Threat Modeling Exercise focused on real scenarios playing out across the channel in 2019 and a mix of recent tactics seen in the wild. The table below summarizes the techniques attackers use that Datto focused on during the case studies. These techniques and IDs are from the MITRE ATT&CK Framework. Additional information can be found at https://attack.mitire.org and is worth reviewing to gain a deeper understanding of how adversaries operate in the real world.

Upon completion of the Threat Modeling exercise, each participant ranked the top five vulnerabilities surfaced during the exercise. The group collectively shared their top five findings and provided guidance on what and where to focus on immediately following the end of the engagement. It was the end of this exercise that all the discussions came together and often provided the *aha!* moments with participants.

The exercises fell short of actually calculating Risk, meaning there was no calculation of financial loss. NIST 800-37 uses the formula "Risk = Assets x Threat x Vulnerability," where Assets have a value that can be lost, and a Threat is the "thing" exploiting the Vulnerability identified. Calculating financial loss is a highly individualized process, and that was beyond the scope of the engagement. The mitigations prioritized for participants were considered foundational security practices, in many cases, basics that apply to all environments. Further discussion on these is found later in this paper.

Threat Modeling

Many formal methods exist for modeling cyber threats against an application, infrastructure, or the business environment. Given the engagement timing, Datto took a less formal approach to the exercise. The Datto exercise involved creating an architecture diagram of infrastructure and services from the Asset Inventory data, identifying boundaries of internal networks, customer connectivity, and integrated connections within the tech stack. In some cases, this process took fifteen minutes and in the larger environments well over an hour to enumerate. In all cases, a full map was never created before by a participant. Figure 2 is an example of a less complicated map. Having created the architecture diagram, we stepped through these scenarios to review the controls in place and enumerate the vulnerabilities that exist for the MSP. Despite taking a less formal approach to the exercise, these discussions proved to be invaluable.

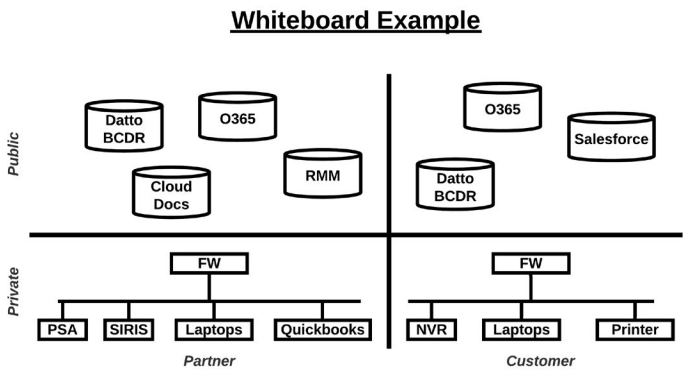

Figure 2

Grey Box Penetration Test

In parallel to the NIST CSF Benchmark and the Threat Modeling exercise, the participants had a tightly scoped Penetration Test as part of the engagement. Taking the collected information in the discovery phase, a senior member of Datto's Penetration Testing team began testing on the participant's infrastructure.

In terms of operating rules, a live Slack channel was open during the exercise and if Datto uncovered something sensitive, a check-in occurred before proceeding. The exercise did not include phishing, given the effort required for standing up the targeted infrastructure for each participant. Finally, while breaking into personal accounts of employees was off-limits, account credentials found in past breaches were in scope to be used against business systems. This is a common tactic used by attackers. In the real world, threat actors do not see a line between the work and personal, using everything they can to meet their objectives.

The workflow followed by the penetration tester was fairly standard. Collected data enabled the first step, enumerating the infrastructure to determine what vulnerabilities exist. While Datto was provided a list of IP Ranges for efficiency reasons, any motivated individual can (and does) enumerate a list on their own. Second, the penetration tester created a list of known employees from websites, social media, and any other source. Various accounts and email addresses were passed through a collection of over a billion compromised accounts, traded on the underground forums. This helped surface compromised credentials and other accounts that might have been missed in the initial research. Lastly, scans of the IP addresses and infrastructure provided a list of possible vulnerability targets to explore for exploitation.

Key Trends

Throughout the case studies, Datto identified several findings that eventually became trends based on the frequency by which they were identified. Some of these trends were informed by the NIST CSF Benchmark summary data.

Figure 3: The visualization provides summary views into subcategory rating scoring, collected through the Benchmarking Exercises.

The three views capture the Capability Claim, Confidence, and calculated Overall Rating, outlined in Figure 1.

- The Subcategories (108) for each were rolled up to their respective Categories (23), with a normalized score between 0 to 1.
- Across all participants, the distribution of the Category scores were mapped to the three views.
- The darker the color, the higher concentration of scores.

False Sense of Security

Across the board, there was a false sense of security across many controls and the overall posture of a participant's environment. The NIST CSF Identify Function helps understand the business environment and guide the risk-based decisions. It was typical for Categories as part of this Function to score higher than the others.

	Category	Capability Claim			Confidence			Overall Rating				
		1	2	3	1	2	3	1	2	3	4	5
Identify	Asset Management	0.3	0.5	0.2	0.5	0.5	0.0	0.3	0.3	0.2	0.2	0.0
Identify	Business Environment	0.3	0.3	0.4	0.6	0.4	0.0	0.3	0.2	0.3	0.3	0.0
Identify	Governance	0.4	0.5	0.2	0.7	0.4	0.0	0.4	0.3	0.2	0.2	0.0
Identify	Risk Assessment	0.6	0.3	0.0	0.8	0.2	0.0	0.7	0.1	0.1	0.1	0.0
Identify	Risk Management Strategy	0.7	0.3	0.0	0.9	0.1	0.0	0.7	0.2	0.1	0.0	0.0
Identify	Supply Chain Risk Management	0.8	0.2	0.0	1.0	0.0	0.0	0.8	0.2	0.0	0.0	0.0
Protect	Identity Mgmt, Auth. & Access Control	0.2	0.4	0.4	0.6	0.5	0.0	0.3	0.2	0.1	0.3	0.0
Protect	Awareness and Training	0.4	0.2	0.4	0.8	0.2	0.0	0.4	0.2	0.1	0.2	0.0
Protect	Data Security	0.6	0.1	0.3	0.7	0.4	0.0	0.6	0.0	0.2	0.3	0.0
Protect	Info. Protection Processes & Procedures	0.5	0.3	0.2	0.7	0.3	0.0	0.5	0.1	0.1	0.2	0.0
Protect	Maintenance	0.5	0.2	0.3	0.5	0.5	0.0	0.5	0.0	0.2	0.3	0.0
Protect	Protective Technology	0.6	0.2	0.2	0.7	0.3	0.0	0.6	0.1	0.1	0.2	0.0
Detect	Anomalies and Events	0.7	0.2	0.0	0.8	0.2	0.0	0.7	0.1	0.1	0.0	0.0
Detect	Security Continuous Monitoring	0.7	0.2	0.1	0.9	0.1	0.0	0.7	0.2	0.0	0.1	0.0
Detect	Detection Processes	0.6	0.2	0.1	0.9	0.1	0.0	0.6	0.2	0.1	0.0	0.0
Respond	Response Planning	0.6	0.2	0.2	0.8	0.2	0.0	0.6	0.2	0.0	0.2	0.0
Respond	Communications	0.8	0.2	0.1	1.0	0.0	0.0	0.8	0.2	0.0	0.0	0.0
Respond	Analysis	0.7	0.2	0.1	0.8	0.1	0.0	0.7	0.2	0.0	0.1	0.0
Respond	Mitigation	0.7	0.2	0.1	0.9	0.1	0.0	0.7	0.2	0.1	0.1	0.0
Respond	Improvements	0.9	0.1	0.0	1.0	0.0	0.0	0.9	0.1	0.0	0.0	0.0
Recover	Recovery Planning	0.8	0.2	0.0	1.0	0.0	0.0	0.8	0.2	0.0	0.0	0.0
Recover	Improvements	0.9	0.1	0.0	1.0	0.0	0.0	0.9	0.1	0.0	0.0	0.0
Recover	Communications	0.5	0.5	0.0	0.7	0.2	0.1	0.5	0.3	0.1	0.0	0.0

Figure 3 - NIST Cybersecurity Benchmark Summary

Similarly, the Protect Function had a higher average, with participants claiming they protected their assets. Protect covers the implementation and maintenance of assets and data, something that aligns very closely with the MSP model.

However, when working through the Threat Modeling exercises the case studies identified that the confidence of controls was lacking and were not always universally implemented.

Basics Overlooked

Attack vectors widely reported in the media were found in participant environments. External exposure of Remote Desktop Protocol, single-factor authentication for VPN and critical cloud services, and reuse of a single credential for all client environments was present despite the significant uptick in the media over the last year.

Gaps Tend to Scale with Size

Datto expected that as an MSP grew in size and revenue that there would be a correlation in the investments to the technology stack.

The thinking was the program would be stronger and more mature as a result. While spending on technology increased, what was surprising is that the maturing MSPs who invested in technology had more exposure due to misconfigurations, data and access sprawl, and systems left by technicians who no longer work at the company. The frequency of these concerns correlated to the size of the tech stack of an MSP.

Tech Heavy and Process Light

The NIST CSF Benchmark Summary shows participants that have invested in tooling had a stronger technology Capability Claim in the Protect Categories, covering things such as Identity & Access Management, Network, and Endpoint Security. The Confidence, however, in these Subcategories were relatively Unsubstantiated. Lower Confidence highlights that implemented technical controls often lacked the supporting processes to ensure effectiveness. Controls such as two-factor authentication (2FA) were inconsistently implemented and firewalls were leveraging default settings. These settings included signatures set to only detect threats and had no activity logging enabled. In discussions with the MSPs, the reasoning

fell into a few categories; limited resources, limited knowledge, or a false sense of security from their technology.

Management of Vulnerabilities

A few MSPs had the ability to run vulnerability scans for themselves, but no MSP performed regular scans of their external\internal infrastructure or had a process in place for remediation. The Penetration Test enumerated several external vulnerabilities across multiple engagements. With enough time, the exploitation of several MSP assets on the internet would be possible.

Exposure to Security Practices

While working through the NIST CSF Benchmark with many of the MSPs, Datto, on average, spent three to four hours to complete the one hundred and eight questions. MSPs required a primer for each Subcategory of NIST CSF and often required walking through the environment for examples for a fulsome understanding. The majority of MSPs later, stepping through the Threat Modeling Exercise helped connect the dots of the missing controls and the net effect on the security program. The engagements highlight a few things. First, MSPs can pick up these concepts rather quickly when presented with the right context and information. Secondly, most MSPs lack exposure to mature security programs, peers, or the ideals of a good program. Lastly, the global cybersecurity talent shortfall that exists hits MSPs as experienced talent migrate towards upmarket roles that command larger salaries.

Detect, Respond, Recover?

As the previous finding surfaced, the majority of MSP attention for NIST CSF focuses on the first and second Categories; Identify & Protect, respectively. What was most surprising is that the Detect, Respond, and Recover Functions receive little to no attention. Outliers here were the MSPs who had an incident that forced maturity in a Category. Additionally, those who had a higher Capability Claim in the Analysis or Mitigation Categories had missing care & feeding or analysis processes when it comes to genuinely satisfying controls. MSPs rely on protective technologies and invest less in detective tools and processes that catch Threats that slip past single layer tools like traditional antivirus.

Supplier Management

When pressed on the Subcategories for Supply Chain Management, MSPs show a high-level of trust for their suppliers. In almost all cases, MSPs have never conducted due diligence of the provider's controls and security posture. MSPs need to approach this with a Trust-but-Verify mindset. Attacks on the supply chain mean technology suppliers, Datto technology included, are targets and vectors for potential attacks. MSPs should perform additional due diligence of the technology and services they are using to manage their clients.

Incident Readiness

When speaking with MSPs on the Subcategories related to Business Continuity and Incident Response, the responses mostly indicated that in the face of an incident, actions would be ad hoc in nature. Meaning, not one MSP had a documented plan (large or small) with the steps for if critical services were not available or an attack occurred. Reasons noted were the size of the staff, lack of time, or being dismissive of the value of such a plan.

Recommendations

The recommendations below are the summary of actions that MSPs should be taking and are a result of the case study's efforts. As noted, the security program of an MSP will be look different based on the risks it faces. Prioritize accordingly, and don't take on the entire list at once.

The Cobbler's Children Need Shoes, Too

The old saying about the cobbler's children having no shoes comes from serving the needs of clients rather than taking care of their own house. The case studies show that MSPs protect their customers more effectively than themselves. Given the rise of targeted attacks on MSPs this should raise concern. These are motivated attackers that are seeking to gain access to meet an objective, in many cases taking over tooling to ransom as many endpoints as possible. MSPs need to ensure their own house is in order when it comes to security to protect themselves and their clients.

Security Requires Continuous Improvement

It is essential to get into the mindset that information security requires continuous improvement. Successful outcomes require more than a set-it-and-forget-it approach. Threats are continually evolving, and what was secured yesterday can be vulnerable today. MSPs should get to a level of comfort with their security posture but never sit back as if it is complete.

Implementing a technology or tool in your environment needs to be more than working through the administration guide. Documentation has a cost in lost time at a client site; it was by far the most common response received. But investing in technology and not receiving the full return on investment is not exactly good business practice. Ensure processes for managing the tools are documented and routinely executed.

Create goals for the program that are reasonable and attainable. Balancing the challenges that come with running a business means prioritizing the things MSPs need to do, and mindfully deprioritizing those that can wait. Information security is no different. When faced with a long list of security improvements, take the top five and work through those until they are complete. Review the list and repeat the process, don't tackle the whole list at once. It's worth noting that it should be an evolving list; it's a continuous process.

Continuous Improvement in Practice: An MSP made an investment in an endpoint detection and response (EDR) platform for their practice. A few months later an MSP hired a managed security service provider (MSSP) to conduct a penetration test of their environment which turned up a handful of problems with Active Directory. In this scenario the MSP should both fix the Active Directory gaps, as well as ensuring that the exact scenario is detectable in the EDR platform in the future. It's the continual improvement to the environment and tools that will lead to better outcomes.

Honesty is the Best Policy

When reviewing your security posture, it does little good to overstate the coverage of your security controls as well as the effectiveness they have in your environment. Being honest and having the dialogue that comes along will lead to better and more secure outcomes. As Datto worked through the engagements with MSPs, participants embraced the findings and worked them into future plans. This provides positive insight into the willingness of MSPs to have the honest conversations.

This recommendation and "Seek Guidance" go hand-in-hand. Enlist the services of a MSSP to conduct penetration testing for your environment to help get an honest, unbiased perspective. Having a third party provides a level of accountability that can be difficult to replicate with just internal staff.

Identity Management

The need to implement 2FA cannot be understated. If a tool used in your tech stack offers 2FA or moving to your single sign-on platform, implement it today. The case study shows that MSPs are leaving critical systems with passwords, API keys, and documentation stores open without strong authentication.

Having accounts to manage the various tools of a tech stack requires multiple logins and keeping track of them all is painful. For solutions that support it, look to implement a unified identity platform that allows you to integrate your solutions into a single identity. Unified Identity shortens your staff on-boarding and off-boarding times and lowers the time each day your techs spend logging into their tools while enforcing a common set of policies.

Not every technology provider supports single single-on, so individual accounts and passwords will be necessary. Ensuring that each account has a different password can be a tedious task, but in the end, it can significantly reduce the likelihood of Credential Stuffing or Password Spraying attacks. There are several channel and non-channel password management offerings. Standardize on an option for your business. There are even options for sharing credentials amongst the team.

As part of the process of gaining access to a target environment, attacks look into personal accounts that someone might have and search out the passwords in breach dumps, just like business accounts. In some cases, your personal accounts are a means to gain access to your worklife. Be sure to use unique passwords and use 2FA on critical personal accounts.

There is an unknown number of underground marketplaces and public services where password information can be purchased. Enlist a service that surfaces the compromised credentials from the dark web so that you can be aware of system compromises. Using the unique password strategy will also help you better identify the source of the credentials.

Move Beyond Protective Controls

Many MSPs include security controls that are primarily preventative. MSPs also gravitate towards controls that are easy to use and have a lower management cost. The more time to manage them, the less time they have to grow the business, so this makes sense. Inherent in this mix of tools are lower false positives, but that opens the possibility of lower detection rates. Detective controls understand that not everything is preventable. They provide insight into the environment that helps surface threats lurking in business systems.

The team over at Perch has created a "Weighted Decision Matrix" for analysis by MSPs that are seeking to move beyond protective controls. You can work through the spreadsheet with any type product or class of control, adjust ratings, and add features or functionality that are important to your business and service offering.

Harden Your Email Services

The case studies conducted surfaced a number of controls gaps when it comes to email security. In the 2019 State of the Channel Ransomware Report, Datto identified 67% of ransomware attacks use phishing as the tactic. MSPs need to take note on the following improvements to help reduce the risks of email delivery:

Implement SPF, DKIM, and DMARC to your business email to significantly improve email security. The case studies conducted surfaced a number of controls gaps when it comes to email security. Spoofing of emails can help attackers exploit trust between MSPs and clients; an individual is more likely to click on a link or open a file from a recipient. The amount of SPAM received by a user also factors into the problem. Higher volumes of email numb and lowers the vigilance one has on vetting phishing emails.

Add an advanced filtering layer to the basic email protection suite included with Gmail or Office 365.

Harden Your Endpoints

There are several things you can do to harden your endpoint devices. Create a standardize secure baseline configuration for your user and server assets and apply these via your RMM. The Center for Internet Security provides some excellent materials on secure standards, apply what makes sense for your environment. If you don't use PowerShell, disable it. If customers don't use Macros, disable them in Microsoft Office. The 2019 Verizon DBIR identified 45% of the malware attacks used a Microsoft Office document as the delivery file type.

An additional resource that is worth reading was released by Ninja RMM in July of this year, 2019 Cybersecurity Checklist: Practical Steps for Securing your MSP Business. This checklist includes a number of endpoint considerations as well as a great list of others worth reviewing.

Segment Your Network

Base the network segmentation approach around the needs of your business. At a minimum, break out the Guest Network onto an isolated VLAN. Having untrusted visitor devices on the network alongside customer management systems is poor practice. For larger or more mature shops:

- Break out server assets and testing labs onto isolated networks.
- Isolate tech workstations from non-tech workstations, server assets from client workstations.
- Segment third party vendor access through VPNs and applied least privileged to the access they have to your network.
- Validate the policies after implementation to ensure effective isolation between segments.

Implement Vulnerability Management Practices

Managing vulnerabilities on the external and internal networks should be a priority. Yet, not a single MSP in the case study had a vulnerability management program internally. Running occasional scans is not enough; successful outcomes require a repeatable and managed process that remediates critical findings promptly.

Be Prepared

The absolute last thing an MSP should be doing during an incident is figuring out what they actually need to be doing. The amount of adrenaline pumping through the body means decision-making processes are affected. Critical actions are timely, and there is little time to decide what to do during an incident. Additionally, Cyber Insurance Policies often have requirements that, if missed, could result in not getting paid out.

Brian Weiss of ITECH Solutions who suffered through a ransomware attack shared "Create an incident response plan, even if it is just a bullet point or a check list. Some of the 25-50 page or overly done incident response plans tend to get glazed over in times of stress." Spending the afternoon with the team on a Friday and think through a scenario such as ransomware hitting your network.

Seek Guidance

Having an experienced CISO on staff may not make sense for most small and medium businesses or MSPs. Virtual CISO (vCISO) services exist to help MSPs understand the challenges and help drive accountability in resolving the gaps in security programs. If a vCISO is too costly, enlist the help of an MSSP to tune and configure the tools and processes. MSPs don't have to do this alone.

Join Security Communities

MSPs can quickly adapt to solve any number of challenges for their clients. Learning security best practices is no different. Reddit has an active MSP community, and within the platform are many options to grow your knowledge, but don't stop there. Many cities have regular events where you can meet individuals, hear talks, and grow your tradecraft.

Another source of experience can come from MSP peer groups. These groups allow the sharing of best practices as well as the war stories from MSPs who have been in the trenches. Seek out and join these MSP peer groups to learn just about anything, including security.

Invest in Staff

The talent shortfall for cybersecurity professionals is a real problem, and finding qualified people is both difficult and costly. If within budget, seek to add experienced security staff to your bench. Alternatively, find existing staff that has a natural curiosity and love problem-solving. Develop these individuals into tomorrow's professionals. Investing in their future helps with retention, and in turn, MSPs can benefit from a better security posture.

Due Diligence of Suppliers

Choose suppliers wisely and don't be afraid to research and ask questions about security practices. Today's attackers are working their way up the supply chain, and you have a responsibility to push your providers as a means to protect your business.

Due Diligence in Practice: MSPs should review their critical technology and service providers through two primary processes.

- When bringing in new technology solutions, create a reasonable list of questions that cover the main areas of concern for your business.
- At a yearly cadence, review your critical vendors to surface any new concerns or to revisit existing concerns.

Notable Findings

Throughout the case studies, Datto identified several findings that weren't necessarily trends across all the engagements but are worth sharing with the community. These are areas that MSPs should review in their own environment and make plans to remediate.

- No 2FA – Not implemented on the following systems: RMM, PSA, Backup & Recovery, Documentation Store, VPN, Cloud Management Portal, Password Management, Metrics Platform
- 2FA Bypass – PSA system with no 2FA with SSO into 2FA protected RMM system
- No Password Manager – Vulnerable browser-based password managers in use
- Reliance on Traditional AV solutions – No use of EDR endpoint or hunting services to look for persistent threats
- Shared Passwords – Reuse of a single credential across all customer sites for administrative or VPN access
- Home Networks – VPNs connected home networks with no ACLs
- Vendor Access – Vendor VPN with complete network access
- VLANs without ACLs – Networks that had VLANs did not apply ACLs with least privileged in mind
- API Reuse – Single API keys used for multiple integrations
- API Privileges – API keys often provided more access than was required rather than least privileged

We Are Stronger, Together

Over the last year, the increase of attacks on MSPs has made a few things clear. First, ransomware is a lucrative business model for cybercriminals and is here to stay for the foreseeable future. The threat of ransomware has the possibility of upending the entire MSP business model and could lead to regulation of the industry if we fail to self-organize. This is an outcome we collectively wish not to see.

Second, MSPs, clients, and the ecosystem of suppliers like Datto have a shared responsibility with meeting the requirements of cybersecurity. It is the combination of people, process, and technology that solves this difficult business challenge. The suppliers in the ecosystem need work more closely, in new ways. Over the last year the partnerships formed like MSP-ISAC and community webinars has been a great start. Additionally, suppliers need to forge ahead with shared open standards that allow better integration with security controls that are consistent across the ecosystem. MSPs need to take the recommendations in this case study and begin to implement better practices. Customers need to be educated that this is a difficult challenge and understand the business risks of not having security included into their managed service offering.

Third and last, people's lives are being affected on an almost daily basis as a result of cybercrimes. Across the industry, MSPs are being attacked with ransomware being the primary threat, as well as a number of other cybercrimes impacting business across the globe. The economic and personal loss makes this a problem that can't be ignored or have ownership slip through the gaps. While the livelihoods of many are on the line, this isn't a hopeless problem. Instead, it's one that requires cooperation. The hope is that the findings from this case study help further the work being completed in the channel and encourages us all to strive a little farther.

Authored by Dan Garcia

datto

Corporate Headquarters
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
United States
partners@datto.com
www.datto.com
888.294.6312

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291

Updated 1 June 2020