THE DEFINITIVE GUIDE TO IT SECURITY

Protecting Your MSP
& Your Customers

liongard™

THE DEFINITIVE GUIDE TO IT SECURITY

Protecting Your MSP
& Your Customers

CONTENT SECTIONS

Is Your MSP Secure from Threats?

When data breaches make the news, it's usually about the big fish—the mega corporations, retailers, financial institutions and organizations that house millions of customers' data or financial records. Less covered are the small- and medium-sized organizations and managed services providers (MSPs) that find themselves under attack every day.

While you might be tempted to think that your smaller MSP is less of a target than a big-box retailer, hackers often target MSPs believing their organizations to be smaller and possessing fewer resources to secure their systems than larger businesses, making it significantly easier to get in and out quietly. Though many MSPs are actually locked down much better than enterprises, the fact remains that the average time to identify a breach is over 200 days—a long and costly period of time for a company of any size. Thankfully, MSPs that haven't already done so have the ability to tighten up their operations to better prevent security breaches with a little forethought and preparation.

In this definitive guide, Liongard contributors **Art Chavez** (Information and Application Security Architect) and **Vincent Tran** (CISSP, Founder and COO) will take you through the various ways your MSP can protect itself and your customers, including:

- → **How to determine which security assessment is right for you**
- → **The differences between security assessments**
- → **The latest security tips to protect yourself**
- → **How you can continue to protect your MSP in the future**

VINCENT TRAN, CISSP

→ SECURITY STORIES FROM THE MSP LANDSCAPE

Your MSP is a Target

ChannelE2E confirms that ransomware attacks have been impacting MSP systems internationally, with hackers breaking into MSP networks, disabling backup and disaster recovery (BDR) systems, and then getting back out to launch ransomware attacks—sometimes waiting days, weeks or even months before carrying out their assaults. Recovery can take weeks, risking lawsuits or complete shutdowns for the MSPs affected.

CYBERCRIMINALS MOST OFTEN LEVERAGE AN ATTACK ON AN MSP IN ONE OF THE FOLLOWING THREE WAYS:

- → **Island Hopping.** The act of using one company as a jumping point to access another, attackers can use this approach to access valuable data that can be held for ransom.
- → **Lateral Phishing Attacks.** By compromising an email account within an MSP, the attacker can then send emails to customers, tricking them into infecting endpoints as part of a larger attack effort.
- → **Fraud.** Networks are browsed to locate and access accounts payable systems. Once cybercriminals know who will be paying you, how much and when, they can spoof an email to your customer pretending to be a member of your accounts payable team.

REMEMBER THE CONTROVERSY SURROUNDING HILLARY CLINTON'S PRIVATE EMAIL SERVER IN 2016?

The MSP that managed the server never imagined itself embroiled in such a scandal. Though the MSP survived the ordeal, they learned a valuable lesson firsthand: **no MSP is immune to a major security investigation**.

OTHER THREATS FACING YOUR MSP:

- → Misplaced/lost external devices (e.g., USB drives or portable hard drives)
- → Phishing/social engineering
- → Software updates not immediately installed
- → Disgruntled/careless employees
- → Poor password management and weak authentication measures

→ SECURITY STORIES FROM THE MSP LANDSCAPE

Debunking Security Myths

MSPs know that security is valuable, but many still fall victim to one or more of these myths:

MYTH #1: CYBERATTACKS ONLY HAPPEN TO LARGE ORGANIZATIONS.
Truth: While organizations of all sizes are at risk, MSPs and smaller organizations often think they're not a target because of their smaller size and lack of resources—ironically, making them a bigger target.

MYTH #2: PREVIOUSLY IMPLEMENTED CONTROLS WILL STILL WORK.
Truth: The only way to properly protect your MSP is to stay up to date on the latest threats and advances in innovative security solutions. Remember, security needs are different for every organization.

MYTH #3: YOU ONLY HAVE TO WORRY ABOUT OUTSIDE THREATS.
Truth: A disgruntled employee could very well cause security issues for a vulnerable MSP, as could a careless mistake by an employee. Paying attention to these security issues within your organization is extrememly important.

MYTH #4: CYBERSECURITY IS ONLY ABOUT PLAYING DEFENSE.
As the public becomes more familiar with security, they expect greater measures to be taken. Showing your commitment to developing and maintaining a strong cybersecurity posture provides peace of mind to current clients and attracts prospective ones who can trust that their data is safe.

Liongard's Actionable Alerts notify you when any deviation from your MSP's standards is detected, letting you stay ahead of security threats and other potential issues. Utilize Liongard's inspectors to review permissions and access rights to audit your own MSP employees when they are added and removed.

DID YOU KNOW?

2/3

of small- and medium-sized businesses have experienced a **cyberattack** in the past **12 months**

Ponemon Institute/Keeper Security

→ **SECURITY STORIES FROM THE MSP LANDSCAPE**

Safeguarding Your MSP

Despite a worrisome outlook on security issues facing the IT industry, you have plenty of ways to safeguard against attacks. ChannelE2E suggests taking the following steps:

- → Embrace Multi-Factor Authentication (MFA)
- → Configure BDR and Security System Alerts
- → Embrace an MSP Documentation Platform
- → Stay Informed
- → Build Your Long-Term Plan
- → Boost Your Employees' and Your Customers' End-User Awareness
- → Integrate Wisely
- → Partner with MSSPs

DID YOU KNOW?

89%

of MSPs state that **ransomware** is the **most common threat** to small businesses.

Datto

→ HOW TO MAKE YOUR MSP STAND OUT FROM THE CROWD

The Benefits of Compliance and Security

Security starts with having standards for documentation (another name for gathering critical and salient configuration data) and standard operating procedures (SOPs)—the ability to trigger and act on discovered anomalies. The MSPs that not only *know* the importance of adhering to security and compliance standards but also take the steps to actually *do* it, and do it *well*, are head and shoulders above their peers in a number of ways because they can:

1. **Better meet customer needs and expectations** by providing consistent and comprehensive insights to customers and demonstrating clear value.
2. **Reduce liability** through automated and standardized documentation, which enables rapid responses to audits and eliminates the blame game when unexpected changes occur.
3. **Increase valuation of their MSP and accelerate growth** with comprehensive and deep depth-of-state configuration information, for higher fidelity visibility into the true surface area of assets, users and systems you manage.
4. **Differentiate themselves from their competitors** by analyzing information across systems and customers to derive standard operating procedures and insights that are unique to their MSP.

DID YOU KNOW?

$7.5 Billion

Cost of U.S. ransomware attacks in 2019

EMSISOFT

Every 39 Seconds

Malicious hackers attack computers and networks

University of Maryland

16.2 Days

Average downtime due to a ransomware attack in Q4 2019

COVEWARE

→ DECISION TIME : MSP + MSSP OR PURE MSP?

Should I Become an MSSP?

A frequent question that arises from MSPs surveying the security landscape—should I continue on as an MSP, or should I become a managed security services provider (MSSP) instead?

ASSESSING THE CURRENT SECURITY LANDSCAPE

Many customers would like their MSP to become a one-stop shop for all IT needs, including security services. To meet these growing demands, some MSPs have chosen to branch out into the MSSP space with tiered offerings or package deals that include security expertise for specific clients. This leads to additional sales opportunities but also comes with increased shared responsibilities and often shifts liabilities to you.

A BLUEPRINT TO MSSP SUCCESS

MSPs today have much richer options for platforms that offer advanced monitoring, change detection and more—and that's where Liongard makes an impact. Its discovery, documentation and auditing capabilities eliminate manual tasks, proactively address critical changes and allow MSPs to keep a watchful eye on their clients' environments. And for MSSPs, it provides that solid foundation of visibility and auditability as to how systems are configured and what changed when, including looking back in time.

PLAN YOUR WORK, THEN WORK YOUR PLAN

Being an MSSP can mean a lot of different things. Don't just jump on the bandwagon because an opportunity exists—"fear of missing out" can't be your driving force. Instead, focus on your MSP's goals, the specific outcome that you want to deliver to customers and what will be uniquely compelling about it—then validate that with your customer base. The type of customers you serve—or those you want to serve in the future—will play a large part in your decision to become an MSSP.

SEIZE YOUR OPPORTUNITIES

Regardless of your decision to offer advanced MSSP services or not, keep in mind your customer already expects a level of foundation security to be baked into your managed services. According to a Continuum survey, small businesses will hold their MSP responsible for security issues—even if their MSP doesn't contractually provide them with cybersecurity solutions. However, that's also a golden opportunity to grow your MSP without making the full dive into becoming an MSSP, as the survey reports that small businesses would pay an average of 27% more for the right cybersecurity offering.

→ START ENHANCING YOUR MSP'S VALUE TODAY

The Importance of Investing in Your Security Position

As you grow and mature as a company, following industry standards and obtaining third-party assessments demonstrate that you're invested in providing the utmost security services and ensuring your customers' information remains protected. The continuity of your MSP depends on not only securing your systems, but also being able to prove that you do so. You'll also gain a competitive advantage over those who haven't invested the time and resources to become a trusted provider.

START YOUR JOURNEY TO ENHANCED SECURITY WITH THE NIST FRAMEWORK.

The National Institute of Standards and Technology (NIST) 800-171 framework provides voluntary guidance to nonfederal contractors and organizations who handle, store or transmit controlled unclassified information (CUI) or covered defense information (CDI). However, NIST is mandatory for any organization that is a government contractor, and its safety measures secure critical information in non-federal systems.

For MSPs who currently or may in the future handle CUI or CDI, adhering to the NIST framework helps you better protect that data, and also shows your customers that you know what it takes to keep their information secure.

NIST provides the gold standard for IT security practices and has five functions: **Identify, Protect, Detect, Respond** and **Recover**.

NIST & LIONGARD: ENHANCING YOUR SECURITY POSTURE

Liongard helps you adhere to all five functions of NIST, so you can enhance your security standards and provide your customers peace of mind.

- → **Identify** risk across customers with automated documentation and standardized data collection.
- → **Protect** your systems by using Liongard to monitor, access and audit users in critical systems like Office 365 and Active Directory.
- → **Detect** changes, anomalies and events with Liongard's timeline feature.
- → **Respond** to issues quickly by setting up custom Actionable Alerts in Liongard, which generate tickets straight to your PSA.
- → **Recover** from threats by taking immediate action based on the unified visibility offered by Liongard.

Next, consider some of the following security, data security, healthcare security and federal assessments that may raise your MSP's credibility.

→ **FIRST STOP: SECURITY ASSESSMENTS**

SOC 2

A System and Organization Controls (SOC) 2 audit provides detailed assurances of an MSP's system controls. The SOC 2 audit is performed by a third-party CPA (AICPA in the United States) who reviews an organization's internal controls and provides an opinion on their effectiveness and security.

A SOC 2 DETERMINES THAT AN ORGANIZATION COMPLIES WITH THE FOLLOWING TRUST SERVICE CRITERIA (TSC):

- → **Security**
- → **Availability**
- → **Confidentiality**
- → **Processing integrity**
- → **Privacy**

THERE ARE TWO TYPES OF A SOC 2 EXAMINATION: TYPE 1 AND TYPE 2.

- → **Type 1:** Focuses on the description of an organization's system and its ability to meet relevant trust services criteria at a specific point in time.
- → **Type 2:** The same as Type 1, but with an additional assessment on the operating effectiveness of an organization's controls over a longer period of time.

DID YOU KNOW?

LIONGARD COMPLETED ITS SOC 2 TYPE 1 IN 2019 AND ITS SOC 2 TYPE 2 IN 2020.

THOUGH RIGOROUS AND COSTLY, IT'S WORTHWHILE BECAUSE:

- ✓ It keeps the PII (personally identifiable information) and privacy of our own employees, leadership and investors secure.
- ✓ It protects our MSP clients' data and provides that extra peace of mind to them as well as their customers.

A company with SOC 2 Type 2 certification, in short, has demonstrated that its systems have been designed and verified to keep sensitive data secure. As more and more businesses scrutinize their vendors' risk management strategies, this certification demonstrates a strong commitment to security on the part of an MSP.

→ FIRST STOP: SECURITY ASSESSMENTS

ISO 27001

The International Organization for Standardization (ISO) 27001 is an information security framework that was created to support organizations of any industry and size. Built around the process of monitoring and improving security to holistically improve an organization's security posture, the ISO 27001 focuses on integrity, confidentiality and availability of an environment's data.

THERE ARE SEVEN MANDATORY CLAUSES AND OBJECTIVES FOR ANY ORGANIZATION SEEKING COMPLIANCE WITH THE ISO 27001 FRAMEWORK:

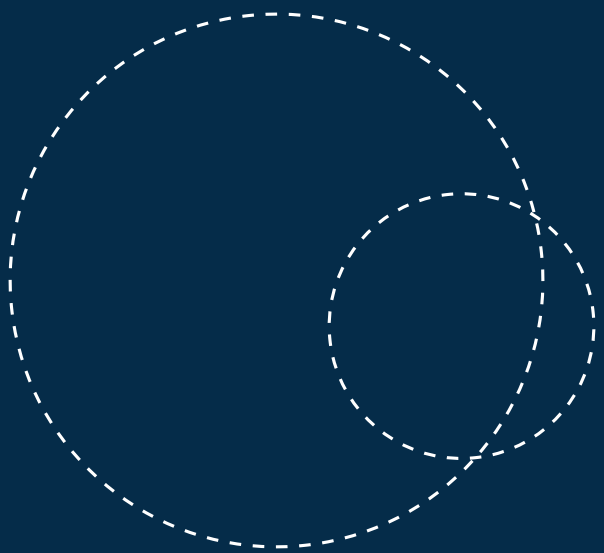
- → Leadership
- → Support
- → Planning
- → Operation
- → Performance Evaluation
- → Improvement
- → Context of the Organization

DID YOU KNOW?

92.4%

of **malware** is delivered through **email**

Verizon



Comparing SOC 2 and ISO 27001

	SOC 2	ISO 27001
What it covers	Detailed historical report that illustrates control activities and system description	A certification of international standard for the management, implementation and maintenance of an information management system (ISMS).
Location	United States	International
Type of assessment	Attestation	Certification
Who verifies compliance	A third-party CPA in the United States (AICPA)	An accredited certification body
Deliverable	Report	Certificate
Performed by	An independent assessor	
Focus	How organizations address information security and mitigate information security risk	
How often it must be completed to remain compliant	Annually	Every 1-3 years, but annually is strongly suggested

→ **LOCK DOWN WITH DATA SECURITY ASSESSMENTS**

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of information security standards for organizations that store, process or transmit cardholder data. The increased controls aim to reduce credit card fraud.

THERE ARE 12 REQUIREMENTS THAT ORGANIZATIONS ARE REQUIRED TO IMPLEMENT FOR PCI DSS COMPLIANCE:

1. Protect your system with firewalls
2. Protect stored cardholder data
3. Use and routinely update antivirus software
4. Configure passwords and settings
5. Encrypt transmission of cardholder data across open/public networks
6. Regularly update and patch systems
7. Restrict physical access to workplace and cardholder data
8. Assign a unique ID to each user with computer access
9. Implement logging and log management
10. Maintain documentation and perform risk assessments
11. Perform vulnerability scans and penetration tests
12. Restrict access to cardholder data on a need-to-know basis

→ LOCK DOWN WITH DATA SECURITY ASSESSMENTS

GDPR

The goal of the General Data Protection Regulation (GDPR) is to give European Union (EU) residents control over their personal data and to streamline the regulatory environment for international business by strengthening and unifying data protection for all EU citizens.

Any organization that handles EU citizen Personal Identifiable Information (PII)—regardless of whether or not they are located in Europe—must comply with the GDPR standard. With U.S. MSPs having the potential to serve customers all over the world, it's imperative to take this standard into your security considerations. Fines for violating GDPR standards can reach up to €20 million (approximately $23 million).

LIONGARD IS COMMITTED TO ENSURING COMPLIANCE WITH GDPR LAWS AND REGULATIONS THROUGH OUR GDPR DATA PROCESSING POLICY.

DID YOU KNOW?

$3.86 Million

Average total cost of a data breach to a business

IBM

45% to 70%

Reduced risk of cyberattacks with an increased investment in employee training

Aberdeen Group

100

Percentage of IT professionals at small businesses who said they could improve their cybersecurity systems

CSO

Comparing PCI DSS and GDPR

	PCI DSS	GDPR
Requirements	Payment card industry's self-regulated standard	Government mandate
Data involved	Payment card data and cardholder information	Any personally identifiable information (PII) of EU citizens
What it covers	Storage, transmission and processing of cardholder data	Any and all processing of personal data
Reporting requirements	No requirement for notifying the public of a data breach	Must report a data breach to supervisory authorities within 72 hours of becoming aware
Handling PII	Businesses must know where cardholder data resides, and keep it encrypted	Requires logs to be kept regarding the processing of any personal data
Parties responsible	Data controllers and data processors	Merchants and service providers
How to become compliant	Demonstrated by undergoing a compliance audit	No formal method

→ **EXPAND YOUR MARKETABILITY WITH HEALTHCARE SECURITY ASSESSMENTS**

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) was designed to define the policies, processes and procedures that are legally mandated to protect electronic protected health information (ePHI). Ensuring compliance with HIPAA is vital for organizations that handle or transmit ePHI.

The healthcare industry will always need MSPs. By not making a concerted effort to adhere to HIPAA regulations, you could be losing out on lucrative opportunities.

Although Liongard doesn't touch or store patient data directly, we choose to be compliant with all HIPAA regulations in order to help our own MSP clients demonstrate due diligence to their healthcare customers.

DID YOU KNOW?

12.55%

of the U.S. population's healthcare records were exposed, impermissibly disclosed or stolen in 2019

HIPAA Journal

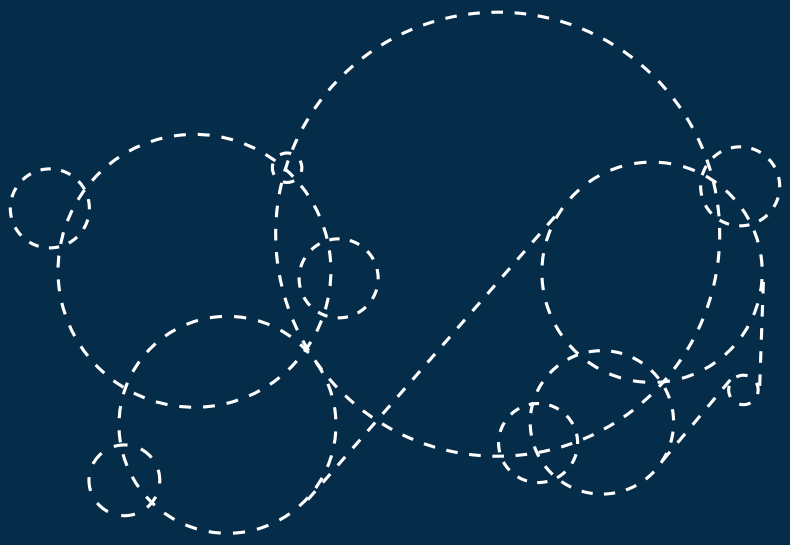
→ **EXPAND YOUR MARKETABILITY WITH HEALTHCARE SECURITY ASSESSMENTS**

HITRUST CSF

The HITRUST Common Security Framework (CSF) was designed for any organization that does business with a healthcare entity. HITRUST CSF offers a comprehensive, certifiable and flexible risk framework. Today, it has moved past its healthcare-focused origins and now can be used for any organization in any industry. HITRUST takes applicable parts of existing standards and regulations and presents them as a "common" framework. Adopting the CSF framework and obtaining third-party certification allows organizations to promote themselves as HIPAA compliant.

THE CSF CONTAINS ELEMENTS OF THE FOLLOWING STANDARDS AND REGULATIONS:

- → **ISO 27001/2**
- → **SOC 2**
- → **NIST Cybersecurity framework**
- → **OCR HIPAA protocols**



→ **EXPAND YOUR MARKETABILITY WITH HEALTHCARE SECURITY ASSESSMENTS**

Comparing HIPAA and HITRUST

	HIPAA	HITRUST
Requirements	Law	Framework
What it is	A set of standards and regulations that protects sensitive healthcare information	HITRUST is the entity that created and maintains control frameworks that include different compliance regulations
Intended for	Any organization handling or transferring ePHI	Any organization that wants to increase their security, regardless of whether or not they are in healthcare
Has a certification	No	Yes
Consequences	Has defined penalties for security breaches	Does not have defined penalties for security breaches

DID YOU KNOW?

3 out of 4

small-to-medium sized businesses say they don't have enough personnel to address security

Ponemon Institute/Keeper Security

→ **DIG DEEPER WITH FEDERAL ASSESSMENTS**

FISMA

The Federal Information Security Management Act (FISMA) of 2002 is a U.S. federal law that requires federal agencies to develop, document and implement an information security and protection program. FISMA:

- → Is required for any organization that is pursuing a contract and an Authority to Operate (ATO) from a government agency
- → Provides clear, defined requirements for maintaining an information security system's data and infrastructure
- → Allows different implementation options based on the severity of the impact from a potential security breach—a unique quality for a security assessment

Possible penalties for government agencies **and their third-party vendors** that fail to comply with FISMA:

- → Censure by congress
- → A reduction in federal funding
- → Reputational damage
- → Government hearings
- → Loss of future contracts

DID YOU KNOW?

4 out of 5

small- to medium-sized businesses report malware evading their antivirus software

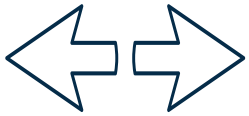
Ponemon Institute/Keeper Security

WHAT ABOUT FedRAMP?

The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security, authorization and continuous monitoring for cloud products and services used by federal agencies. While not often utilized by MSPs, a full FedRAMP examination is necessary for any organization providing (or hoping to provide) cloud products or services to federal agencies.

→ DIG DEEPER WITH FEDERAL ASSESSMENTS

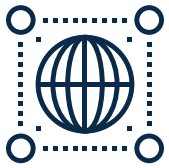
Comparing FISMA and FedRAMP



	FISMA	FedRAMP
What it is	A set of standardized guidelines government agencies use to protect sensitive data.	A program that standardizes the approach to security assessments, authorization and cloud service provider monitoring.
Applies to	Products hosted on premise for government agencies.	Products hosted on the cloud for government agencies.
Requirements	FIPS 199, FIPS 200, NIST SP 800-53	FedRAMP modified NIST SP 800-53 standards, FIPS 199 and FedRAMP-specific documentation and templates
Assessment	Any auditor who is authorized to access information systems	An accredited Third-Party Assessment Organization (3PAO)

→ **MORE WAYS TO BEEF UP YOUR SECURITY PRACTICES**

Using CIS Controls to Mitigate Risk



Because you can never take too many precautions when it comes to security, the Center for Internet Security has put together simplified guidelines to help IT professionals protect their businesses and customers from cyberthreats. The CIS team's 20 Critical Security Controls offer prescriptive actions you can take to reduce risks. The controls are broken down into three categories:

1. **Basic CIS Controls,** which should be implemented in every organization for cyber defense readiness.
2. **Foundational CIS Controls,** a step up from the basic CIS Controls and smart for any organization to implement.
3. **Organizational CIS Controls,** distinct from the others and focused more on people and processes.

USING LIONGARD TO SUPPORT CIS CONTROLS

With fresh, automated system data, Liongard provides visibility into customer environments to monitor for critical changes. Plus, alerts can be set for just about anything you want to keep an eye on.

We've matched many of Liongard's alert rules to the specific CIS controls they help support. For instance, we have approximately 25 alerts that support ***CIS Control #1: Inventory and Control of Hardware Assets***, including "Active Directory workstations at or near the end of support."

→ MORE WAYS TO BEEF UP YOUR SECURITY PRACTICES

Taking a Proactive Approach

Just because you've completed a security assessment, mitigated risk and defined and closed any existing security gaps, doesn't mean that you're done. Review these additional steps you can take to ensure your MSP stays secure:

- → Educate and train employees frequently
- → Undergo compliance assessments regularly
- → Monitor news and stay updated on security advancements and changes
- → Update systems and software frequently
- → Design and implement formal security and privacy policy procedures
- → Design and implement privacy and security controls
- → Create a BYOD (Bring Your Own Device) policy for employees to follow

SECURE, COMMUNICATE, REPEAT

An MSP that puts security at the top of its list gives customers and prospects peace of mind. Share with them all that you do to mitigate security risks.

For more on how Liongard continually builds trust through transparency and compliance, visit our Trust Center.

DID YOU KNOW?

44%

of businesses estimate they could lose $10,000 or more during just one hour of downtime

Infrascale

24x

The average cost of downtime compared to the average ransom amount

Datto

33%

Total costs related to a data breach that accrue one year or more after the event

Upguard

$6 trillion+

The estimated annual cost of global cybercrime damages by 2021

Cybercrime Magazine

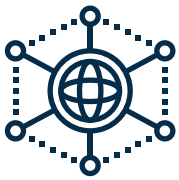
→ TAKING THE RANSOMWARE TARGET OFF YOUR BACK

Keys to Avoiding Ransomware Attacks

Instead of being low-hanging fruit, mitigate your risks of ransomware attacks by following best practices:

- → **Activate and enforce MFA:** With cybercriminals becoming more skilled at accessing credentials, it's imperative to have MFA enabled for all users. Additionally, a privileged access management (PAM) process can help minimize lateral movement and damage done if a bad actor does penetrate your system.
- → **Restrict network access:** Limit access rights on each employee account to only what they need to perform their jobs—and audit those permissions regularly.
- → If your staff members change, be sure to update access immediately to curtail any possible issues. In addition to enabling MFA, passwords should meet strong requirements, be updated regularly and never be recycled.
- → **Prioritize patching:** When a vendor releases an update to fix a vulnerability in their software, install that patch immediately—before it's too late.
- → **Secure endpoints:** Malicious emails still account for many ransomware attacks, so make sure to employ email authentication and web filtering tools as well as antivirus software. More importantly, ensure that every endpoint is protected, and virus definition libraries are up to date.
- → **Set alerts:** When you properly configure your systems so that you receive alerts when settings are changed, you're able to operate proactively and stay ahead of threats. Liongard is one way to be automatically notified about system changes.
- → **Use off-site backup:** If an attacker has compromised an MSP's RMM software, it probably also has access to the MSP's backups. That's why, in addition to two separate backups on-site, you should also have a third, off-site (and, preferably, offline) backup that only a few key people have access to for enhanced security.
- → **Document, revisit, repeat:** Make sure you have a system where you store your data protection and cybersecurity processes, disaster recovery plans and other emergency guidelines, and review them with your team on a regular basis.
- → **Stay informed:** Sign up for security alerts issued by the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency to stay current.
- → **Protect yourself:** Following the NIST Cybersecurity Framework and implementing CIS Controls help minimize risk in your MSP, so you can help your customers do the same.
- → **Educate your team and end users:** Training your team and your customers to avoid and detect cyber threats can go a long way in mitigating ransomware attacks. Furthermore, encourage users to share information of detected social engineering and electronic cyber threats with colleagues to increase awareness. Avoid shunning victims as it may lead them to obscure details that can help alleviate future ones.

Layering Your Defense



MSPs must take their own security seriously, implementing the same layered defenses they provide for their customers.

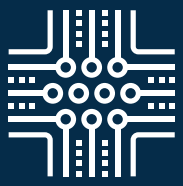
DEFENSES SHOULD INCLUDE PROTECTION AT THE FOLLOWING LAYERS:

1. **(Logical) Perimeter –** The perimeter today largely consists of email coming in and users going out to browse the web. Putting DNS, web and email scanning in place will minimize the number of threats that can make their way onto your network.
2. **Endpoint –** Putting an antivirus on endpoints to stop viruses and malware is necessary for stopping known threats.
3. **User –** Your employees are either part of your security stack or enablers of attacks. Enrolling them in continuous security awareness training will elevate readiness for potential attacks, suspicious web and email content, and obvious tactics they may encounter, ensuring your employees don't become the reason for a successful attack.
4. **Privileged Access –** Attackers need elevated access to move around your network and/or your customers' networks. Having some form of privileged access password vault for all credentials which provide such access will help to reduce the risk of compromised accounts.

Source: ChannelE2E

→ **STANDARDIZE. SECURE. SCALE.**

How Liongard Can Solidify Your Security Foundation



Security and compliance are vital for MSPs to take seriously and implement, but can also absorb a lot of time, money and focus from MSP leaders. At Liongard, we're committed to advancing IT industry knowledge and to helping MSPs automate essential processes such as continuous discovery and change detection, documentation and reporting on key metrics. With more process automation, MSPs have more standardized and accurate data, better visibility into changes within environments, and the ability to detect, identify and address security concerns early. Further, in the event of a compromise, the ability to have deep configuration documentation is invaluable—enabling rapid root cause analysis and reducing time-to-recovery. This automation frees up valuable time for MSPs to focus on activities to scale their operations, including building high performing sales teams and providing more proactive, value-adding customer service and support.

Liongard's innovative platform was purpose-built to empower MSPs through automated solutions to **standardize**, **secure** and **scale** operations.

TO LEARN MORE ABOUT HOW LIONGARD CAN HELP YOUR MSP'S SECURITY AND COMPLIANCE JOURNEY, VISIT LIONGARD.COM.

→ CONTRIBUTORS

THANK YOU!

We hope you enjoyed this guide to enhancing your MSP's security. For automated documentation, actionable alerts and reporting and metrics to drive your MSP business forward, look no further than Liongard.

→ **Art Chavez, CEH, OWASP, Information & Application Security Architect, Liongard**
With 20+ years in IT, including the past several years focusing on IT security and compliance, Art has seen the industry change, grow and trend toward increased vendor risk management. At Liongard, he works to ensure that not only is the company practicing due diligence to stay secure, compliant and trustworthy, but it's also finding ways to address the security concerns of MSPs and their customers.

→ **Vincent Tran, CISSP, Founder and COO, Liongard**
In 2017, Vincent co-founded Liongard to help managed services providers automate discovery and documentation of critical systems configurations so they could become more efficient and profitable. He has more than 20 years of experience as a cybersecurity expert, web application and information architect and online marketer.