

Building Cyber Resilience Against Ransomware

January 2021

LOCKTON®

AUTHOR(S)



Timothy K. Smit
CIPP/E, CIPP/US, CISSP
Global Privacy &
Cyber Risk Consulting Leader
1.303.414.6011
timothy.smit@lockton.com

Over the past year, ransomware attacks have increased exponentially. In some reports, the figure is reported as a 700% increase since March 2020.[1]

Adding to the complexity of the ransomware difficulties, on Oct. 1, 2020, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) issued an advisory regarding potential sanctions for facilitating ransom payments. That same day, the Financial Crimes Enforcement Network (FinCEN) issued an advisory on ransomware and the use of financial systems to facilitate payment. Our summary of the Advisories and attendant issues can be found here.[2]

Given that ransom payments may no longer be a viable option or, at a minimum, paying a ransom to threat actors may be more difficult, organizations need to lay a strong foundation to increase their resilience against ransomware attacks. A keen focus on preventing, identifying, responding, and recovering is crucial.

What can organizations do to minimize their risks of ransomware attacks?

On Sept. 23, 2020, the National Institute of Standards and Technology (NIST) published Special Publication (SP) 800-53, Revision 5, entitled Security and Privacy Controls for Information Systems and Organizations.[3] The SP contains 20 security and privacy control families. While we won't address all 20 control families in this article, we have highlighted several prioritized and focused controls that should be considered and potentially implemented by organizations from a ransomware loss control perspective.



THE CONTROLS BELOW WILL ALSO MAP TO POSSIBLE QUESTIONS INSURANCE CARRIERS ARE STARTING TO ASK IN THEIR CYBER APPLICATIONS. These questions aim to better understand what proactive controls have been implemented at your organization, which may make you a lower risk to them.

With more people working remotely, the increase in endpoint devices for organizations to manage and protect continues to grow. Following the cyber kill chain model,[4] here are a few ways to help your organization protect itself.

Identifying and containing the incident is critical. According to the 2020 Ponemon Institute Cost of a Data Breach Report, the average time to identify and contain an incident was 280 days.[5] That number has risen due to workforce members working remote and not necessarily identifying or reporting an incident to their organization.

Implementing tools and processes that protect your workforce and their endpoint devices is where we will begin.

A few of these tools and processes include:

- Intrusion detection and prevention systems
- Endpoint detection and response tools
- Multifactor authentication
- Disabling of remote desktop protocols and gateways

There are several proactive solutions to consider implementing to help build resiliency into your organization's infrastructure and operational processes.

Training & education

One of the most common ways ransomware is launched within organizations is through a phishing attack. Train and encourage your workforce to report anything suspicious in real time. Your incident response teams need that information as soon as feasible to confirm the integrity of your systems and start their investigation on how and where an attempt to infiltrate originated, so they can respond immediately and potentially eradicate the possibility of further attempts.

Organizations should consider recurring security trainings across their workforces, presented on their primary means of communication, i.e., desktops, laptops, mobile devices or smartphones. Focused training delivered on these easily accessible devices will help your workforce identify phishing attempts on their main communication tools.

Technical controls

Endpoint protection

Technical controls for different endpoint protections that remove the likelihood of your organization succumbing to a targeted attack. Those include:

- Implementing prescreen links in emails
- Scanning for files with exploits
- Stripping and detonation of attachments

These controls protect your organization if malware circumvents your current controls by identifying those infected files, attachments, etc. Expediting your response to these threats allows you to contain incidents sooner, decreasing the probability of infected files cascading and propagating throughout your network, both internally and externally.

Network segmentation

Network segmentation indirectly self-contains malware from cascading to your entire organization, reducing the overall possible business interruption impact.

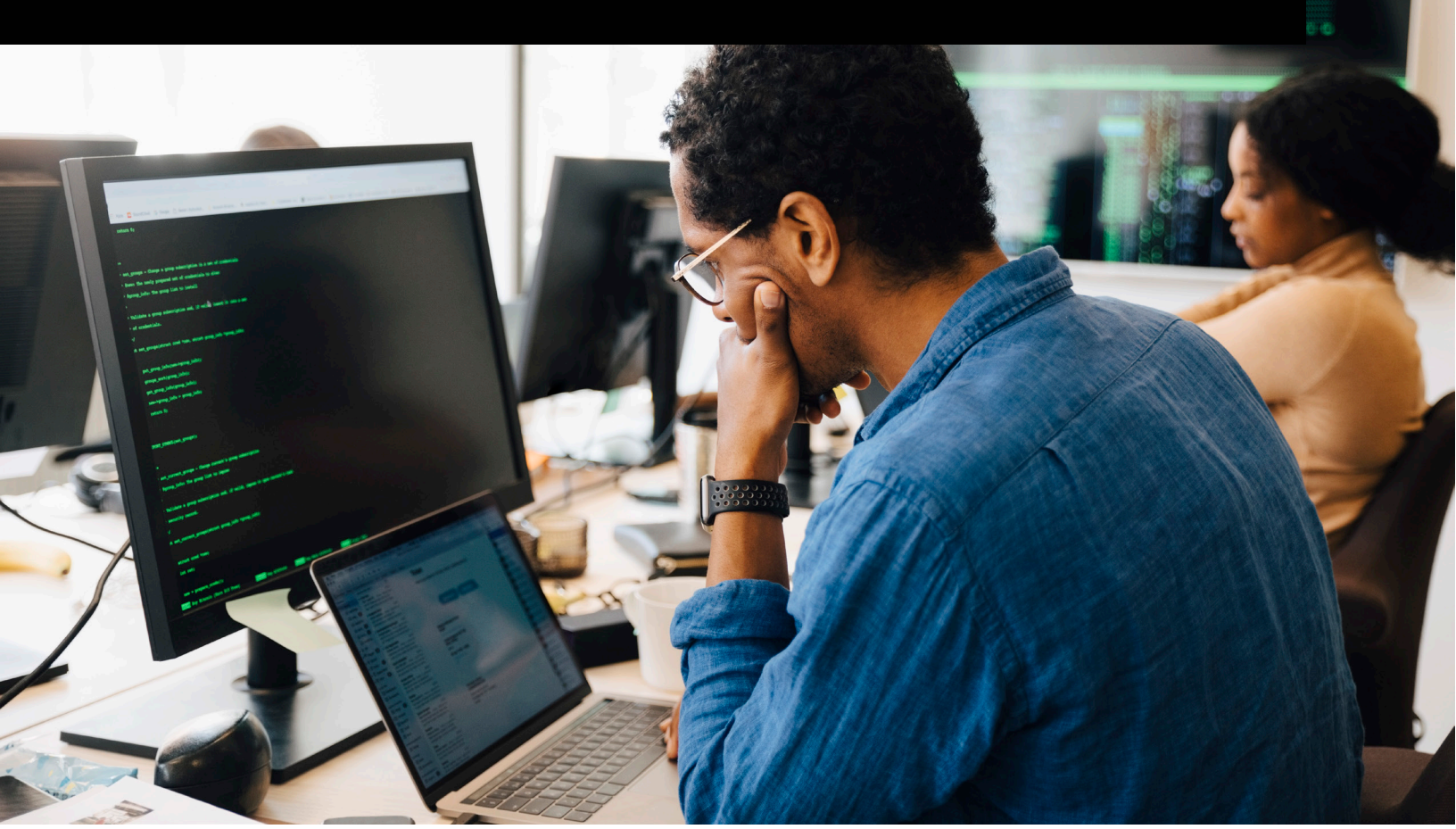
An example of network segmentation is of a large organization with multiple offices across the globe. The organization's security policy restricts those office employees from accessing its financial reporting system, both locally and globally. Network segmentation can enforce the security policy by preventing all office traffic from reaching the financial system. With the prevention of that traffic which also provides a reduction in overall network traffic, the financial system will work better for the financial analysts who utilize it.

Vulnerability management

The implementation of configuration management, a patch management program, and intrusion detection and prevention systems alerting your security operations center (SOC) provides a quick reactionary force to engage and contain abnormal activity before it becomes a larger issue.

Digital footprint detection

Vulnerabilities exploited by the threat actor leave a digital footprint within your networks and should be captured, investigated and acted upon, where needed. Those efforts are improved by implementing security event logging solutions, applying threat intelligence to those events, and analyzing behaviors captured.



Data inventories & data maps

Data inventories and data maps of information flow paths aid your organization in classifying critical data while overlaying the proper controls to protect that data based on its data classification. The data is classified by importance to business operations and organizational goals and objectives. It provides your organization with a prioritized list of critical systems and assets to protect most data being proactively backed up and protected while the data is at rest.

A data inventory also sheds light on end-of-life (EOL) systems, operating systems, etc. that currently do not have additional security updates or patches available. Using EOL systems exposes your organization at a much higher rate to new threat agents.

That vulnerability may make your organization noncompliant with regulatory requirements that explicitly state you must protect your network and data. One example of that is the U.S. HIPAA Security Rule, 45 C.F.R. § 164.308 (a)(5)(ii)(B), states that the entity must have protection from malicious software. This implies a need for patches across all systems. Another example is the global PCI DSS standards that require each entity to develop and maintain secure systems and applications by installing applicable vendor-supplied security patches.[6]

Article 32, Security of Processing, within the General Data Protection Regulation (GDPR) states that the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Data backups

Data must be backed up and protected from unauthorized access and alteration or deletion with a tested restoration plan that empowers your organization to be resilient to cyber-attacks, including ransomware attacks. Backups may be locally conducted and stored, or they may be virtual within a cloud environment.

Authentication controls

Multifactor authentication

Implementing multifactor authentication (MFA) is critical to confirm the identity of those accessing your systems and/or devices. For example, if your organization utilizes MS Office 365 (O365), MFA implementation is free and available today to implement. If your organization does utilize O365, ensure that the Advanced Threat Protection add-on is being utilized. MFA should be applied to protect every account, including privileged accounts.

If you allow work emails to be forwarded to personal email accounts, ensure that your workforce has enabled MFA on their personal accounts, especially in today's work-from-home setting.

Even though MFA will not prevent phishing emails from being clicked on or executed, it can reduce by over 90% the number of phishing attempts that successfully exploit login credentials.[7]

Cyber insurance carriers

Organizations that currently purchase a cyber liability insurance program with Lockton have access to all the above-mentioned recommendations and many other services that are provided either as complimentary or at a reduced cost. Insurers are helping their clients proactively improve their overall risk posture while reducing the probability of a cyber event causing a loss, which triggers a claim.

Lockton's privacy and cyber risk control services are available to help identify and prioritize needs, and subsequently assist in addressing those needs.

Please contact your Lockton Cyber & Technology Practice Associate for further information to assist your organization with risk control solutions tailored to your organization's business needs and objectives.

Glossary

CONFIGURATION MANAGEMENT Configuration management is a system's engineering process for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design and operational information throughout its life.

END-OF-LIFE (EOL) End-of-life (EoL) is a term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life (from the vendor's point of view), and a vendor stops marketing, selling, or rework sustaining it. (The vendor may simply intend to limit or end support for the product.)

PATCH MANAGEMENT Patch management is the process that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones.

SEGMENTATION OF NETWORKS Network segmentation is an architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. This allows network administrators to control the flow of traffic between subnets based on granular policies.

References

1 https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

2 https://global.locktonco.com/news-insights/office-of-foreign-assets-control-warns-against-paying-cyber-ransoms-to

3 https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

4 https://www.varonis.com/blog/cyber-kill-chain/

5 https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/

6 https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

7 https://www.knowbe4.com/how-to-hack-multi-factor-authentication



UNCOMMONLY INDEPENDENT

 | © 2021 Lockton Companies. All rights reserved.