110 Horizon Drive, Suite 210, Raleigh, NC 27615
919.459.2081

Cybersecurity and Ransomware

Approved by the PRIA Board of Directors

July 21, 2021

www.pria.us

PROPERTY RECORDS INDUSTRY ASSOCIATION

Copyright Notice, License, Disclaimer
For
PRIA Completed Work Product

August 2021

A. **COPYRIGHT NOTICE**: Copyright © 2021 – Property Records Industry Association ("PRIA"). All rights reserved.

B. **LICENSE:** This completed PRIA work product document (the "Completed Work") is made available by PRIA to members and the general public for review, evaluation and comment only. PRIA grants any user ("Licensee") of the Completed Work a worldwide, royalty-free, non-exclusive license ("License") to reproduce the Completed Work in copies, and to use the Completed Work and all such reproductions solely for purposes of reviewing, evaluating and commenting upon the Completed Work. NO OTHER RIGHTS ARE GRANTED UNDER THIS LICENSE AND ALL OTHER RIGHTS ARE EXPRESSLY RESERVED TO PRIA. Without limiting the generality of the foregoing, PRIA does not grant any right to: (i) prepare proprietary derivative works based upon the Completed Work, (ii) distribute copies of the Incomplete Work to the public by sale or other transfer of ownership, or (iii) display the Completed Work publicly. Comments on the Completed Work must be sent to PRIA.
Any reproduction of the Completed Work shall reproduce verbatim the above copyright notice, the entire text of this License and the entire disclaimer below under the following header:

This document includes Completed Works developed by PRIA and some of its contributors, subject to PRIA License. "PRIA" is a trade name of the "Property Records Industry Association." No reference to PRIA or any of its trademarks by Licensee shall imply endorsement of Licensee's activities and products.

C. **DISCLAIMER:** **THIS COMPLETED WORK IS PROVIDED "AS IS." PRIA AND THE AUTHORS OF THIS INCOMPLETE WORK MAKE NO REPRESENTATIONS OR WARRANTIES (i) EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT; (ii) THAT THE CONTENTS OF SUCH COMPLETED WORK ARE FREE FROM ERROR OR SUITABLE FOR ANY PURPOSE; AND, (iii) THAT IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. IN NO EVENT WILL PRIA OR ANY AUTHOR OF THIS COMPLETED WORK BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES FOR ANY USE OF THIS COMPLETED WORK, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR OTHER DATA ON ANY INFORMATION HANDLING SYSTEM OR OTHERWISE, EVEN IF PRIA OR THE AUTHORS OR ANY STANDARD-SETTING BODY CONTRIBUTORS TO THIS COMPLETED WORK ARE EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.**

Table of Contents

Executive Summary

Many types of organizations are being targeted by ransomware and the attacks are increasing in frequency and sophistication. Some organizations that have paid the ransom have not been fully restored as promised. Other organizations, choosing not to pay the ransom, have spent much more time and money than originally estimated to restore their systems. In both situations, there is the risk of confidential information that was obtained by the perpetrator being sold or released. The disruption to services is in itself costly. The potential for ransomware attacks is a threat to government and business entities of every size and in every physical location. Every organization must consider a reasonable and justifiable cost to protect itself.

This paper provides background information and sets a knowledge-based level playing field. It includes best practices to **protect** against an attack and procedures to follow when an organization **is attacked** by ransomware or other cybersecurity threat. A list of websites where you can find current information is included and are updated by their publishers (see Ransomware Resources).

This paper shares information from organizations that experienced confirmed ransomware attacks.

Participants in this work project included recorders from small- and medium-sized counties, IT specialists, preservation specialists, Land Record Management System (LRMS) vendors, title plant operators, and security specialists.

As you read this paper, it is important to remember that ransomware attacks are evolving and will continue to do so. This paper represents a moment in time.

This document guides government and business professionals in gathering the necessary information to communicate with their technical support provider(s). It makes recommendations on what the technical support provider should do to secure the organization's systems, files, and records.

The cybersecurity principles presented in this paper will protect organizations from various forms of malware.

Understanding Ransomware

How Does Ransomware Work?

Ransomware prevents or limits users from accessing their system and data by encrypting the system's files or network until a ransom is paid. In some instances, the attack is initiated at the point a link is clicked. In other instances, the perpetrator will gain access to the system and download files prior to executing the encryption.

Some type of communication, usually in the form of an on-screen pop-up, appears with a demand that a ransom be paid by using "untraceable" forms of currency (e.g., cryptocurrencies, like Bitcoin).

There is no practical way an organization can secure its information systems to completely eliminate the possibility of a ransomware attack, but the organization can lower the possibility of becoming infected by implementing good cybersecurity practices. If your organization is affected by ransomware, having robust cybersecurity measures in place will allow for a quicker recovery with minimal loss to data/information.

The rate of ransomware attacks in the United States is growing every year[1]. In fact, phishing attacks "which are the main driver of delivering ransomware" are growing more than 350 percent annually, while becoming more sophisticated all the time. [2]

Types of Perpetrators

Faced with the growing rate of attacks, protecting your systems and the data from these threats has become even more challenging and complex, especially as organizations transition to a remote workforce.

An organization can be compromised by a range of perpetrators. Below are the types of perpetrators and their motivations.

1. Insider Attack – someone who is contracted or works inside an organization
    A. Financial gain
    B. Grievance
    C. Targeted
2. Hacker – a general term for someone attempting to gain unauthorized access to an organization's network
    A. Bragging rights
3. Opportunistic Cyber Criminal – someone engaged in unauthorized activity with malicious intent
    A. Financial gain
    B. Opportunistic

[1] The State of Ransomware in the U.S.: Report and Statistics 2019 (https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/)
[2] https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine

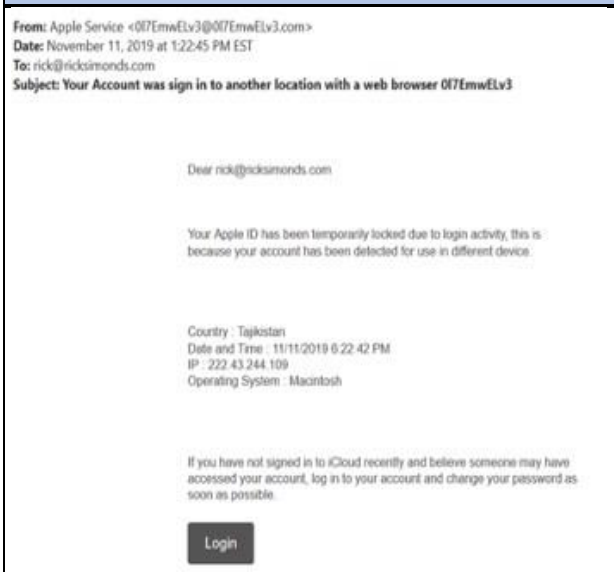
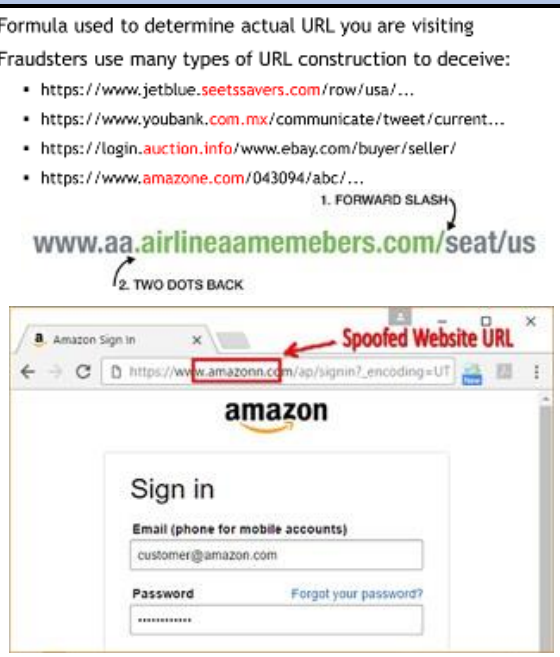
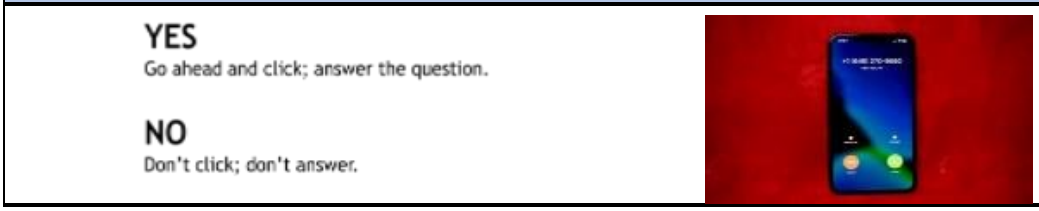
4. Cyber Hacktivist – someone who uses hacking to bring about political or social gain
    A. Grievance
    B. Targeted
5. Cyber Terrorist – someone who carries out a sophisticated, premeditated attack on computer information systems
    A. Political warfare
    B. Targeted
6. State Sponsored – a foreign government carries out a sophisticated, premeditated attack on computer information systems
    A. Political warfare
    B. Targeted

Types of Threats

Below are the most likely current ways that an organization could be compromised by a threat actor or ransomware. The attacks can be targeted or random. Both are opportunistic in nature.

1. Social Engineering
    a. Individual – posing as an employee/contractor
    b. Phishing and Spear Phishing – appearing as a legitimate business or service either randomly or to a targeted group
    c. Vendor spoofing – posing as a vendor on a service call
    d. IT spoofing – posing as internal IT department staff
    e. Website spoofing – creating phony websites that appear to be legitimate
    f. Phone spoofing – cloning a phone number that is familiar (e.g., same area code or local prefix)

    Some pictorial examples from the above varieties of social engineering appear next.

Phishing and Spear Phishing – appearing as a legitimate business or service either randomly or to a targeted group	Vendor spoofing - posing as a vendor on a service call
	
IT spoofing – posing as internal IT department staff	**Website spoofing – creating phony websites that appear to be legitimate**
	
Phone spoofing – cloning a phone number that is familiar (e.g., same area code or local prefix)	
	

Click here for the original presentation from which these types of attacks were excerpted.

2. Cloud Service Providers – Attackers may target a cloud service provider to gain access to customers' network and intellectual property.
3. Unknown/incomplete software and hardware inventory – Without an up-to-date and comprehensive list of all hardware and software, the organization will have difficulty performing patch management to secure internal systems.
4. Insider threats – A user, using authorized access, intentionally exploits, steals, destroys data, or compromises the network and communications.
5. Connecting unknown USB devices – Attackers target organizations by infecting USB devices and leaving them by common access areas where employees will notice them. If the USB device is connected, the attacker can infect the organization's computers and network.
6. Improper firewall configuration – Without a properly configured firewall, your infrastructure will not be protected from malicious network traffic.

Best Practices & Prevention Measures

This section presents best practices to assist your organization in addressing cybersecurity concerns.

Educate Your Staff

In order to protect your organization, it is critical to educate your staff; not just once but routinely as cybersecurity concerns evolve. The momentary lapse by one employee is all that is necessary to affect the entire organization. It is equally important to make sure that your managers make a commitment to on-going training and awareness.

User Awareness – Quick Tips:

1. Pay attention to web addresses you are typing or to which you are being directed.
2. Hover over every hyperlink to verify the validity of the link before clicking. On emails with attachments :
    a. Before clicking on any attachment received, ask yourself "Am I expecting this?"
    b. Is it normal for your job function to receive this type of attachment?
    c. Do you trust or know the source from which the attachment is coming?
    d. Does the email address match the name of the supposed sender?
3. Visit only websites that you trust will not damage your computer. Updated versions of browsers provide tools for identifying trusted websites by reputation.
4. Be mindful of what you share on social media.
5. Alert IT of any phishing emails or questionable sites, so they can investigate and take action.
6. Contact your helpdesk when in doubt.
7. Opt in for multi-factor authentication (MFA) for personal devices and applications.

Management Commitment to Ongoing User Awareness:

1. Conduct security vulnerability assessments to lower your internal risk by identifying weaknesses that could allow attackers to target unsuspecting or uninformed employees.
2. Provide cybersecurity awareness training for all employees on an ongoing basis. Consider third-party educational resources (see Ransomware Resources).
3. Conduct ongoing testing and monitoring, including extra testing for repeat offenders, including phishing tests.

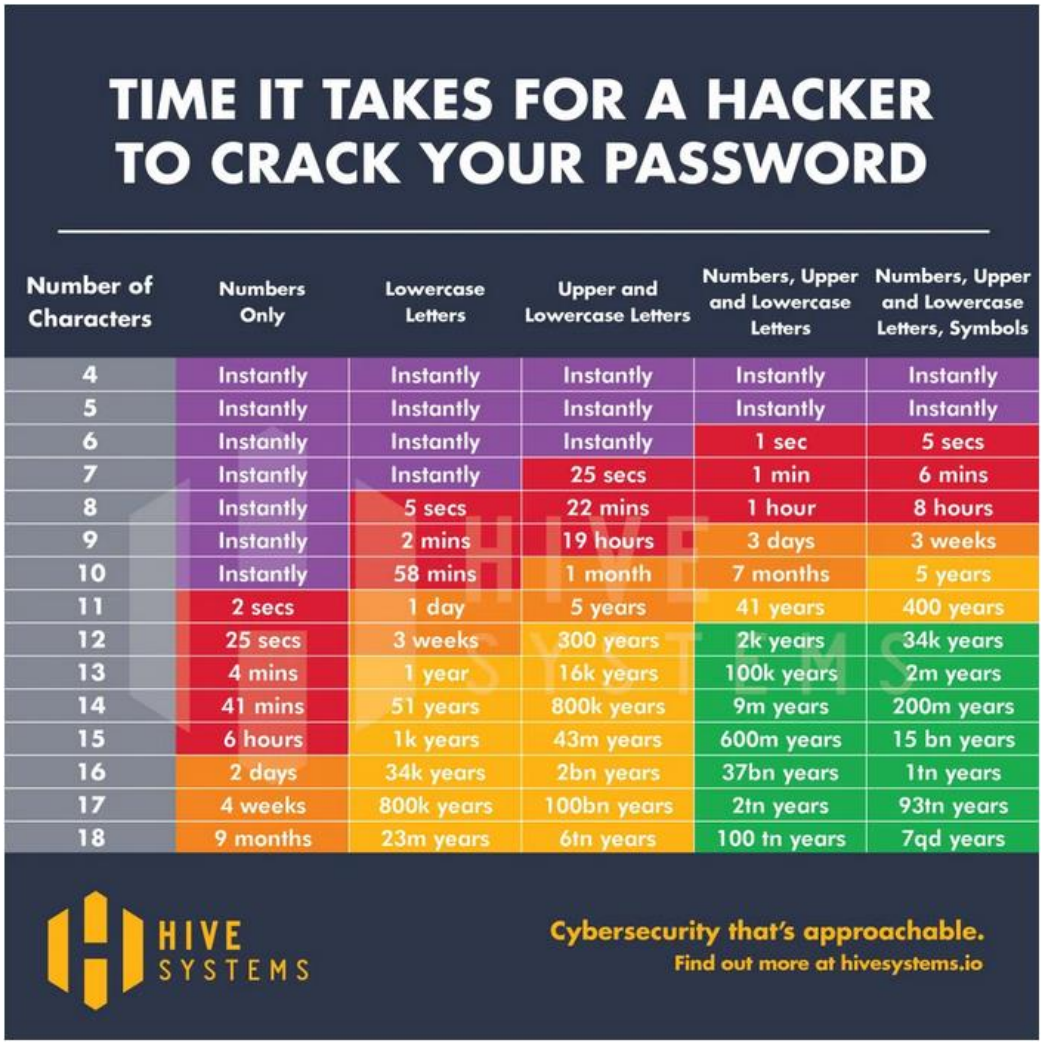
To learn more about educating your users, see the additional options in the Ransomware Resources.

Protecting Systems

It is important that senior management be committed to the investment of time and money necessary to protect your organization. If your managers do not understand what your IT staff is trying to accomplish, the staff will not receive the time or financial support needed.

Below are some of the best practices to strengthen your organization's defenses.

1. Password Policy – Current best practice is to use a password with a minimum of 16 characters, containing upper and lower case characters, numbers, and special characters. The chart on the following page illustrates possible timeframes for cracking passwords with the proper tools.



1. Inventory Management – Know what you own so you can protect it.
2. Software Management – Know what port protocols are needed, and limit access unless needed." Patch Management – Keep your systems and software up-to-date.
3. Encryption – Determine what data needs to be protected from unauthorized access.
4. Multi-factor Authentication – Verify users' identities by requiring multiple login credentials.
5. Credential Management – Secure service accounts. Establish a process for continued business needs for a user account, if the user transfers to a different department or leaves the organization's employment.
6. Principle of Least Privilege – Limit access user rights to only what is necessary to perform their jobs.
7. Backup Data – Maintain redundant copies of your data with a scheduled backup strategy.
8. Real Time Network Visibility – Use tools that monitor all aspects of network processes in real time (i.e., holistic visibility).
9. Threat Detection/Alerting – Identify and notify IT staff of anomalies on the network.
10. Centralized Reporting – Send logging reports to a central location for analysis.
11. IP Restriction – Restrict internet connection coming from/to an unauthorized device.
12. Software Restriction – Control the programs that can run on a computer.
13. Site Blocking – Restrict network communication to unauthorized websites.

14. Network Segmentation – Separate the internal network into segments and restrict what is allowed to move from one segment to another.
15. Firewalls – Implement internal and external firewalls to allow or block communication flow.
16. Enterprise Risk Assessment - Perform an internal risk assessment on a regularly scheduled basis.

Prevention Measures

System Security Maturity Model Concepts

In all areas of IT configuration, development, implementation, and maintenance, there are continuum models designed to help professionals guide their organizations from an initial brilliant idea through development, implementation, and optimization. Each organization will likely find itself at a different starting point on the continuum presented below but it all begins with a complete inventory of the current state of hardware, software, and processes in place. Some processes may be "Basic" or even non-existent while others may already be very "Mature." This continuum endeavors to provide a pathway to get your organization optimized and (as much as possible) to prevent vulnerability to ransomware. Each level represents an increase in cost and sophistication to prevent cyber-attacks. Organizations should assess the services they need and can afford.

	Service	Basic Level	Advanced Level	Mature Level
BASIC	Endpoint malware/ransomware protection.	X	X	X
	All system and desktop patches kept up to date.	X	X	X
	Maintain active licensing for all software and equipment.	X	X	X
	Backups are not stored in a network drive share.	X	X	X
	Use of a security conscious Internet Domain Name System provider (e.g., OpenDNS, Umbrella). Many solutions provide content filtering, phishing protection, reputation-based filtering, domain aging, and other security services.	X	X	X
	Ongoing IT security training for all users based on roles.	X	X	X
	Password manager software that generates unique, complex passwords and requires their use.	X	X	X
	Create and use a hardened baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices.	X	X	X

	Service	Basic Level	Advanced Level	Mature Level
	Routine restoration and recovery of key server(s)' configuration and data form backups.		X	X
ADVANCED	Multi-factor Authentication (MFA).		X	X
	Enhance firewall protection with such features as block list filtering, Intrusion Prevention System (IPS), content filtering, reputation-based URL filtering.		X	X
	Disallow non-authorized devices on the organization's network (e.g., BYOD (Bring Your Own Device), rogue routers).		X	X
	Where possible, implement cloud technology including hybrid solutions for anytime, anywhere access with appropriate credentials, access rules, and enhanced security. Examples include Google Docs and Microsoft Office 365.		X	X
	Partition (segment) the network into multiple subnetworks and enforce rules for communication between them.		X	X
	Penetration testing and vulnerability scans.		X	X
	Multi-tiered incremental backup topology for both application and data not accessible by network shares or end users (i.e., ensure data integrity from overwrites of bad data). For additional information on backup and preservation, read PRIA's paper on Electronic Records Preservation.		X	X
	Ongoing phishing and malware awareness training for everyone in the organization. Create a phishing email address for reporting potential threats to the Help Desk.		X	X
	Use encryption where applicable including backups, databases, hardware, servers, laptops and mobile devices.		X	X

	Service	Basic Level	Advanced Level	Mature Level
MATURE	Further, enhance firewall protection with more advanced features such as application security monitoring. Allow list filtering, advanced IPS configurations, DNS Sinkhole.			X
	Tiered rules for network access (e.g., user, supervisor, manager, director, admin, super admin). Examples include: 1) Users do not have administrator rights to their PC; 2) System administrators use alternate logon when doing admin work.			X
	Endpoint Protection (EPP) or Endpoint Detection and Response (EDR).			X
	Network monitoring software to confirm that network activity is within accepted norms (e.g., SolarWinds, Spiceworks).			X
	Security Information and Event Management (SIEM).			X
	Backups that are stored in a way that requires time and processes to affect those backups (e.g., offsite storage of backup media with third party for retention, using a cloud backup provider that disallows the change or deletion of backups, off-premise application and data hosting).			X

Cybersecurity Insurance

Consider obtaining cybersecurity insurance for the organization. Cybersecurity insurance allows the organization to mitigate losses from most cyber incidents. The incidents do not have to be exclusively from ransomware attacks. It could also be business interruption or network damage. The organization can and should always review the coverage documentation. Acquiring cybersecurity insurance allows an independent organization to review the organization's process and recommends the adoption of different preventative measures that were not previously implemented.

If the organization applies for cybersecurity insurance, be prepared to answer in-depth questions about your staff training, system protections, and system security maturity.

Incident Response

The capability to respond quickly is necessary for ransomware or other cybersecurity threats. A quick response allows the organization to minimize damage and restore services promptly. The response needs to be systematic and immediate. Extensive planning is required to create an effective Computer Security Incident Response (CSIR) plan. Here are a few recommendations:

1. Create or update your CSIR plan and establish a Computer Security Incident Response Team (CSIRT).
2. Create procedures for incident handling and reporting.
3. Establish lines of communication between response teams both internal and external.
4. Determine what services the incident response team should provide.

When an incident occurs, make sure to:

1. Follow the CSIR plan.
2. Record all actions taken.
3. Preserve the forensic evidence.
4. Isolate all impacted systems.
5. Communicate with leadership and ask for help, if necessary. Most organizations cannot handle a full on cybersecurity incident by themselves. There also might be a legal obligation to report the incident depending on the organization.
6. Investigate the incident.
7. Identify the scope/impact of the incident.

Restoration and Recovery

Every government and business organization's disaster recovery plan should address the unique aspects of restoration and recovery from a ransomware/cybersecurity attack. For the property records industry, external organizations may not completely understand and appreciate the operation, obligations, and role in establishing and maintaining the land records that support the transfer of real property. The need to have these records available, on demand, even during a ransomware/cybersecurity incident, requires additional consideration and planning.

Have a conversation with your IT professionals to provide them with awareness and education about your business, the rules and regulations you follow, and the commitments you have to your customers.

Planning to protect these essential records from a cybersecurity attack and providing full recovery is complicated and costly but necessary.

The following questions need to be answered during the restoration and recovery phase of a cybersecurity/ransomware incident.

1. Do you pay the ransom?
2. If you do not pay the ransom, do you try to remove the ransomware or rebuild the systems?
3. Are there lessons to be learned to minimize future risk?
4. Could implementation of different security and technical controls prevent a future incident?
5. What additional risk-based cybersecurity investments is your organization prepared to make?

To answer these questions, an enterprise-wide risk assessment should be completed.

Service Level Agreements

Organizations should have Service Level Agreements (SLA) with their hardware and software providers. For more in-depth information about what an SLA should contain, click here.

Cloud Solutions

Cloud services play an ever-growing role in today's computing environment. There are many types of cloud-based solutions. Many organizations have found cost-effective benefits when using a cloud-based service for infrastructure, backups, and even cloud-based applications. As with all technologies, improper configurations can lead to increased vulnerabilities to the organization, which can compromise the protection put in place to prevent cybersecurity incidents. There have been cybersecurity incidents where a threat actor exploits a relationship between the organization and a cloud service provider.

Benefits of using cloud- based services:

- Offers a good option for backup storage service, as they are physically isolated from the local network and provides additional protection when configured correctly.
- Ensures a logical separation (of both hardware and software) between the local infrastructure and cloud infrastructure.
- Offers multiple locations in which to store data for disaster recovery benefits.
- Implements scalability of services for the need of the organization.
- Allows you to work off-site for business continuity needs.
- Provides anywhere, anytime access to be able to work off-site for business continuity through purchase of redundant internet connectivity resources.

When properly configured, cloud-based services ensure the implementation of System Security Maturity Model Concepts.

Risks of using cloud based-services

Despite the many benefits and protections offered by cloud services, many of the same risks that are present in a local network need to be addressed in a cloud environment. Recent high-profile incidents have shown that more cyberattacks are targeting cloud environments. In these scenarios, hackers have taken advantage of gaps in protection, unclear team responsibilities, and cloud security knowledge. A cloud solution may be as vulnerable as a local network if the cloud service is not properly configured. Appropriate data protections must be in place. Any concerns identified with local area networks should be reviewed with prospective cloud service vendors to mitigate these issues.

Real World Examples

Here are the consequences considered by a county with population of 177,000, which was shut down by a ransomware attack.

In February 2017, all of this county's government offices were completely shut down, including the police force, by ransomware until they paid the ransom in Bitcoin.

The county's offices remained open, but employees didn't have access to telephones or the internet. Even 911 dispatch workers operated without phones or computers.

The table below shows how the county evaluated the impact to determine whether to pay the ransom or undertake the recovery themselves.

Pay the Ransom	**Don't Pay the Ransom**
Roughly $28K	Roughly $275K
Bitcoin	Down time; loss of productivity
No guarantee you won't be hit again	Had the backups to restore
Hackers often keep a backdoor key	Able to put in place manual systems in several departments
Additional cost for upgrades and defenses	Many upgrades and defenses already in the budget
No guarantee that all files will be returned	

A second jurisdiction's attack was quite different. In March 2020, this county's government was shut down because of a cyberattack. The malware had resided in the county's computer system since the previous December but was not deployed until March. The county implemented its COOP Plan (Continuation of Operational Procedures). It was not clear whether there was a complete and accurate backup that could be used to restore the system and files.

Calls were made to the county's Land Records Management System, disaster recovery, imaging, and grab-and-go kit vendors. Grab-and-go kits were assembled including a laptop, receipt and label printers, scanner, mobile printer, APC backup, and data networking hardware.

Once up and running, the county:

- Upgraded server Operating Systems to the latest version
- Applied system configurations to servers, laptops, and desktops
- Implemented a firewall between the county and key business partners
- Implemented Multi-Factor Authentication (MFA) for privileged users
- Initiated Microsoft Office 365
- Established VPN access.
- Implemented third-party 24/7/365 security monitoring
- Limited user access across the enterprise

- Established multi-instances of core services (local and cloud)
- Revised the county's Disaster Recovery Plan

All of this was happening in the midst of a global pandemic with strict distancing standards and limited office personnel in place.

Servers were rebuilt, which took three weeks, and the office was again using its software solution on April 1, 2020.

In hindsight, this county learned that each of these lessons was essential. Every jurisdiction would benefit from implementing these lessons learned.

Conclusion

Ransomware is a growing, evolving, and an increasingly sophisticated threat to every business and government organization. While it costs time and money to establish procedures and protections, these upfront costs are much less than those needed when, not if, a ransomware attack occurs. In order to protect all records, the record keepers need to have frank and in depth conversations with the IT staff. The IT staff needs both financial support to protect the records, and management support to implement many of the protections, which may create some "inconveniences." Line staff may balk at the extra steps needed, but regular testing and alerting software is critical.

Do not delay; start evaluating and evolving your organization's recognition of ransomware's ferocity and your protection measures today. It cannot be overemphasized: your organization needs to be constantly vigilant and prepared.

Definitions

Allow list filtering - an access control mechanism that denies everyone access, except for the members of the allow list.

Block list filtering - an access control mechanism that allows everyone access, except for the members of the block list (i.e., list of denied accesses). Inappropriate content can be filtered by identifying specific websites or by filtering content (e.g., gambling, terrorist sites, pornography).

Domain Name - an easily memorized name for a website or other service on the Internet.

DNS (Domain Name System) - the structure that routes data traffic over the Internet or a private network using a numeric IP address, which identifies the associated endpoint on the network. In part, this routing is accomplished by translating readily memorized Domain Names to the associated IP address.

DNS Sinkhole - A **sinkhole** is a **DNS** provider that supplies systems looking for **DNS** information with false results, allowing an attacker to redirect a system to a potentially malicious destination.

Endpoint - a computing device that communicates back and forth with other devices connected to a private network or the Internet. Examples include servers, personal computers, mobile devices, or any other device with network connectivity.

EDR (Endpoint Detection and Response) - an integrated endpoint security solution combining real-time continuous monitoring and rules-based automated responses.

EPP (Endpoint Protection) - software that protects a network by ensuring compliance of endpoints, such as desktops, laptops or mobile devices, that connect to the network, to prevent installation and propagation of malware (e.g., SolarWinds, Carbon Black, firewall add-on).

IP (Internet Protocol) - A set of rules governing the format of data set over the internet or other network.

IPA (Intrusion Protection System) - a network security threat prevention tool that examines network traffic to identify malicious activity, record and report detected threats, and take preventative action to prevent vulnerability exploits. IPS can be a standalone product or a feature with most firewall systems (e.g., Barracuda, CheckPoint, Cisco, McAfee, Palo Alto, Trend Micro).

Malware - software designed to disrupt, damage, or gain unauthorized access to a computer system. Malware is a general term that covers different types of threats including viruses, spyware, worms, trojans, rootkits, ransomware, etc.

MFA (Multi-factor Authentication) - verify users' identity by requiring multiple credentials (e.g., sending an authorization code as a text message).

Ransomware - malicious software that prevents or limits users from accessing their system and data by encrypting the system's screen or files until a ransom is paid.

SIEM (Security Information and Event Management) - software that collects event logs from various sources such as firewalls, servers, domain controllers and anti-virus software, and then identifies, categorizes and analyzes the events in order to take appropriate action. Examples of software products include LogRhythm, QRadar and Splunk.

Resources

For a list of ransomware resources, click here.

For a list of Service Level Agreement (SLA) considerations, click here.