Guidacent®

GUIDACENT SPECIAL ADVISORY

Ransomware Defense & Recovery Plan

Guidacent®

Ransomware Defense & Recovery Plan

ran•som•ware *(noun)*

1. a type of malicious software designed to block access to a computer system until a sum of money is paid.

2. results extend beyond damage and destruction of data or monetary loss and encompasses theft of intellectual property, productivity losses, and reputational harm.

A major threat. With the advent of war in Eastern Europe and the support of state actors, the threat of ransomware attacks impacting local businesses as well as industry leaders, is becoming very real!

Your Guidacent Ransomware Defense & Recovery Plan can minimize the potential impact of a cyber attack.

Ransomware attacks continue to cause tremendous impact to financial operations and reputations for organizations across all sectors. And the attack patterns being used are becoming more complex as well, as individuals and small businesses are being more widely targeted for ransom by threat actors.

In a recent review of ransomware activity from the summer of 2021, HHS/DHS tracked the top five ransomware threat actors, and with more than 68 percent of the attacks from this year, the bulk of the trouble landed on the doorstep of medical facilities and manufacturing.

And the current state of affairs in Europe continue to raise concerns across the world's business infrastructures.

The trend in ransomware attacks is no longer about some kid in a basement, trying to impress his girlfriend with parlor tricks. Threat actors are well organized and often tied to state-funded organizations, with the objective of gaining access into sensitive assets and holding those assets hostage for millions of dollars.

But "Fear" doesn't fix problems, and planning and preparation can offer a proven defense plan.

As we continue to see this pervasive problem threaten the business landscape, patterns of activity are beginning to trend that are pointing to common threads of risk, which should be addressed as part of a general "Good IT Security Hygiene" to improve cyber defense, which will ***lower the risk of impact from a Ransomware event.***

Guidacent®

PHASE 1

CYBER TRIAGE

Stop the bleeding first, then we'll circle back and rebuild the defenses!

If you are currently experiencing a malware incident or ransomware attack, the following information is your best strategy for minimizing the damage.

7-STEP TRIAGE SUMMARY — DO THIS NOW!

1. If you have an Internet Service provider, contact them immediately.
2. Determine which systems have been affected and isolate them from the rest of the network.
3. If you are unable to disconnect devices from the network, shut down their power.
4. Review those systems that have been impacted to determine how to best get them back up (and clean from infection).
5. Restoration processes should be based on order of sensitivity, urgency and impact to the business or your customers.
6. Contact state and federal authorities and share your findings.
7. Notify your customers.

Your first action should identify those systems impacted and immediately ***remove*** them or isolate them from the rest of your operating environment.

If there are multiple systems or subnets affected by this attack, ***take the network offline*** at the switch level. You may not be able to disconnect individual systems as the event takes place.

If taking the network temporarily offline is not immediately possible, locate the network cable and ***unplug affected devices*** from the network or disconnect their Wi-Fi connection to stop the potential spread.

Once the incident has begun, threat actors may monitor your organization's communications and response activities to assess whether their actions have been detected and/or impacted (and how), by your responses.

Be sure to isolate systems in a coordinated and well orchestrated manner (based on your Business Continuity / ***Disaster Recovery Plan***) and consider using external communication methods (i.e., phone calls, WhatsApp or text messaging), to avoid alerting the wrong people of your activities.

Prioritize systems for restoration procedures and confirm the type of data that may be present on those systems affected (make sure you are using you have ***clean backups***).

Using a critical asset list that you have already defined, your restoration efforts will follow a logical order of priority, based on critical assets. (i.e., systems essential for health and safety, revenue, or ***critical operations***.

Be sure to consult your entire staff team to capture a comprehensive view of the events that have taken place, based on the evidence.

A ***Root Cause Analysis*** will help you as well as legal resources address and mitigate any further risk of compromise.

Guidacent®

PHASE 2

DEFENSIVE PLAN

Stop the Infection, Recover the Assets!

Ransomware is commonly delivered through email phishing campaigns, exploit kits, web-based attacks, and through malicious advertising. Once you've stopped the bleeding, it's time to stop the infection from spreading…

9-STEP DEFENSE SUMMARY

1. Conduct routine port & vulnerability scans
2. Enforce complex password requirements
3. Implement two-factor authentication (wherever possible)
4. Schedule consistent system patch cycles.
5. Disable unnecessary services
6. Ensure your network is segmented as a disruptive defense measure
7. Follow system hardening guidelines
8. Centralize security logging on a protected log collector
9. Implement a security incident and event management (SIEM) system

Zero-day Attacks are surfacing. Many ransomware attacks do not require a user to launch an attack. The Sodinokibi ransomware attack, for example, used a disclosed vulnerability in a database application to download ransomware to an affected server and launch an attack, before a patch was released to stop it.

Use the following to assist in your path to containment and remediation:

1. Review protocols/processes/procedures for updating software and operating systems with the latest patches.
2. Firewall Configurations to block access to known malicious IP addresses.
3. Validate the effectiveness of your system's spam filters (and whether they are fully distributed throughout their system).
4. Ensure your Backup procedures are in place and that you maintain "clean copies."
5. Review the procedures for restricting Internet activity relating outside of the workplace.
6. Ensure your IT administrator or ISP is "whitelisting" your application inventory.
7. Investigate how/if/whether there are Restricted User Permissions (relating to installing and running software applications), and whether/if "Least Privilege" is being implemented.
8. Keep user access privileges restricted, which will impact the movement of potential threats–especially malware.
9. Be sure to scan all incoming and outgoing emails for potential threats and quarantine all suspicious or "anonymous" or rogue messages.
10. Monitor your system for Anomalies

Guidacent®

PHASE 3

ASSESSMENT

Harden the system, Return to Business!

Perform a risk assessment to identify any security weaknesses and vulnerabilities in your systems and address any threat exposures that may be revealed.

SECURITY AWARENESS IS ESSENTIAL!

1. Reinforce company policies regarding not sharing or revealing user credentials.
2. Encourage the use of company-sanctioned file-sharing programs, rather than via email attachments.
3. Adobe Acrobat Reader and Microsoft Word often contain unpatched vulnerabilities that can be exploited.
4. Explain incident reporting procedures and ensure that users feel comfortable reporting security incidents.
5. Automatically enable firewall, advanced malware protection, encryption, and data loss prevention on all endpoints.

Five Questions to Consider… While we know the malware problem continues to burden every business type and throughout all sectors, Consider the following issues when evaluating your defense strategy:

1. **Are we validating everything?**

   By design, and unlike other attacks, ransomware often takes temporary residence on a computer with "Authenticated" credentials, which avoid detection before its encryption algorithm completes its objective

2. **Do we have the right tools *(and are we using them properly)*?**

   Effectively segregating your network and ensuring your endpoint protection controls are properly deployed, will have a powerful impact on defending the edge of your systems.

3. **How do we decide who gets access?**

   Organizations can no longer trust a user because they are an employee (or say they are) or based on their password alone. Zero Trust is a concept based on the impetus that trust is never presumed until proper authentication has been verified.

4. **Did we lock the front door?**

   Review all firewall configurations to confirm all non-essential activities are blocked. Consider subscribing to an OSINT reputation service to automatically block access to known malicious actors.

5. **What didn't we fix that needed fixing?**

   Patch Management: Vendors provide fixes to known and exploitable vulnerabilities. Make it a point to implement the fixes and be sure that all systems and software are current with respect to their patching and updates.

Guidacent®

PHASE 4

RECOGNIZE THE RISKS

Know where the signs of trouble may be hidden in your environment!

To safeguard businesses against ransomware and other attack situations, the first order of business should be understanding the process for how these attacks can exploit processes you may or may not have in place.

Focus on a Risk-centered Cybersecurity Defense

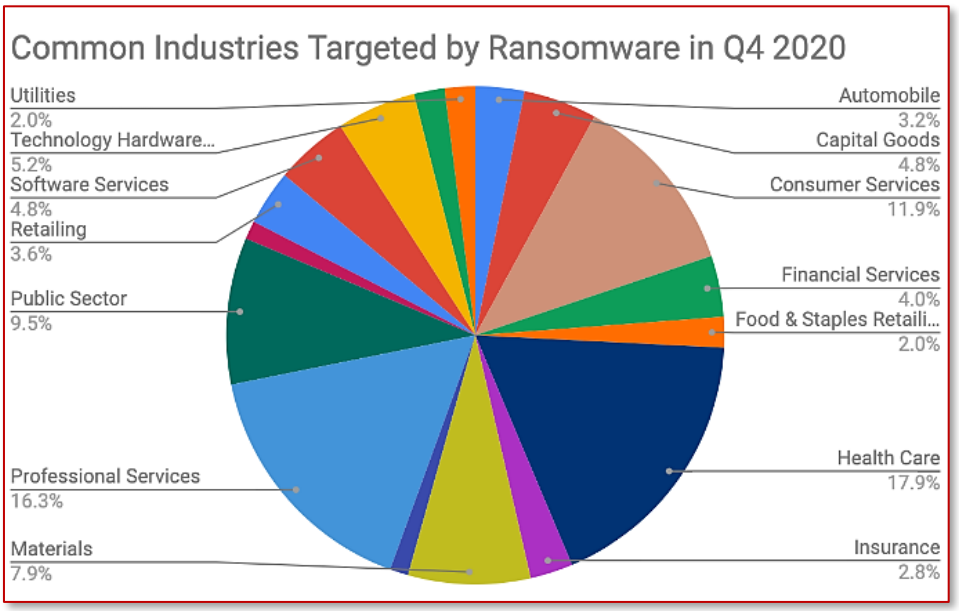
Organizations often face the paradox between paying for tools that seldom get deployed properly and hiring security people who may not be aware or qualified to address relevant needs.

In a ***risk-centered defense*** approach to managing cybersecurity-related activities, two points of reference emerge as essential success factors:

First, the approach focuses on reducing risk as a primary objective, allowing businesses to prioritize their capital investment and corresponding resources, predicated upon cyber initiatives aligning with the ability to reduce risk.

Second, a risk-centered approach classifies key objectives into specific, measurable outcomes as directed by senior executives.

Focus remains on designing and implementing processes and controls that provide the broadest coverage. Yielding the greatest impact to critical operations.



Guidacent®

PHASE 5

ASK THE EXPERTS!

Guidacent's ThreatRecon Security Professionals can help get you in a safer posture to defend against a Ransomware event!

You CAN improve the overall threat defensive posture of your computing environment against these pervasive exploits, which as far as we can tell, are not going to get any easier!

How to Evaluate RISK

- Is the Risk **Timely**?
- Is the Risk **Relevant** to business operations?
- Is the Risk **Pervasive** and capable of spreading?
- Does this Risk pose an **Urgent** impact to the business?

Ready to learn how Guidacent can help your business **establish** a strong Cybersecurity **Defense**?

Email us at

cybersecurity@Guidacent.com

to schedule a free consultation.

Addressing the growing risk from a Ransomware event goes beyond identifying who's looking into your business operations—they may already be present.

For many organizations, becoming resilient to ransomware attacks requires more than incremental improvements. It requires organizational transformation that broadens the scope of involvement at the top of the organization and instills focus on business risk, rather than technology controls.

The ability to focus your investments on mitigating likely outcomes, becomes essential, based on a broad understanding of attacker motives and the ability to anticipate high-impact scenarios.

The consulting teams at Guidacent view cybersecurity and risk management as components needed to better enable businesses to build strong, secure operating environments, which extends the value of our digital infrastructure and economy.

If your organization would like to explore how to evaluate and address risk and build on the integrity of your critical assets, contact us at **cybersecurity@guidacent.com**.

We can help you on the journey and keep you out of dangerous traffic as you're following your business path.