Ransomware Guidebook

Preparation and Response

P.O. Box 1353
E. Northport, NY 11731
978-480-0890
cyber@securityinsecurity.com
www.securityinsecurity.com

There are over 600 million ransomware attacks every year

Ransomware 101

Ransomware, as the name implies, is malicious software (malware) that prevents the legitimate usage of a computer system through the implementation of weaponized cryptography. Typically propagated through phishing email campaigns, social engineering tactics, and/or the exploitation of system vulnerabilities, ransomware is designed to encrypt a victim's file system until such a time that a ransom is paid. Unfortunately, since many bad actors require ransom payments in the form of anonymous cryptocurrency transfers, there is no guarantee that paying a ransom will result in the safe return of system functionality.

Throughout the past decade, ransomware has been steadily increasing in both frequency and impact and is unsurprisingly not limited to any one industry or business sector. According to the National Cyber Threat Intelligence Integration Center (CTIIC): although a majority of ransomware attacks were aimed at commercial entities between 2022 and 2024[1], there was a marked increase in attacks against the healthcare and emergency services sectors as well, which had significantly higher impacts on infrastructure than those against commercial organizations.

Of more notable concern is the fact that the United States is consistently the most targeted country for ransomware attacks by a sizeable margin. Both the population density and the availability of computing resources throughout the country are likely contributing to *some* data bias in this case, however the fact remains that the United States infrastructure and commercial environments are under persistent attack from a faceless enemy with unbelievably powerful resources.

The idea of "reversing" or "cracking" the encryption associated with a ransomware attack is something that even highly trained and heavily funded research laboratories struggle to achieve, since the encryption standards available to hackers today are impressively robust and incredibly fault tolerant. Essentially, once a system is locked out, the only thing capable of unlocking it is the key, and the holder of those keys (the malicious actors) want their money.

---

[1]September 2024, Office of the Director of National Intelligence, "Worldwide Ransomware Attacks as of June 2024 Consistent with Previous Year", https://DNI.gov

Although all ransomware attacks generally follow the same thematic tenets (regardless of implementation strategy), no two ransomware attacks are the same, which makes it particularly difficult for cybersecurity experts or even the Federal Government to carry out any investigative or repercussive actions. Ultimately, this provides an unsettling degree of anonymity for the perpetrators, and when paired with the lucrative nature of the exploits themselves, makes ransomware attacks a go-to approach for hackers.

The Cybersecurity and Infrastructure Security Agency (CISA), The Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST), and just about every other alphabet soup agency under the Federal umbrella have taken the same hardline stance on their recommendations for responding to a ransomware attack… "don't pay".[2, 3, 4]

The 'substantive' rationale that has led to the overwhelming endorsement of this position is largely anecdotal and does not always take into consideration the variability of attack types, target selection process, or method of compromise.

Underlying Theory[3]:

1. Paying does not guarantee a release of the victim systems
2. Paying rewards bad behavior and supports a criminal enterprise
3. Paying once increases the likelihood of being attacked again
4. Making a payment could lead to additional extortion

Unfortunately for many however, "don't pay" offers very little actionable guidance and serves as a disheartening blow that evokes feelings of hopeless panic as desperate victims are left scrambling to figure out what can be done to recover their data. The harsh truth is that once a ransomware attack has been executed, there is very little that can be done to reverse the clock, but that does not mean that all hope is lost.

---

[2]Federal Bureau of Investigation: "Ransomware", www.fbi.gov

[3]Cybersecurity and Infrastructure Security Agency: "Ransomware", www.cisa.gov

[4]National Institute of Standards and Technology: "Preparing Your Organization for Ransomware Attacks", www.csrc.nist.gov

What does ransomware look like?

Ransomware is rarely one-size-fits-all, and tactics have evolved significantly over the years; both in application strategy and use cases. Although there are countless implementations of ransomware throughout the current cyber landscape, there are some common archetypes that are worth exploring in greater depth. Putting aside the fact that there are numerous deviations and variations of these specific ransomware attacks, the following categories represent common varieties of ransomware that are frequently utilized or emulated.

1. Crypto Ransomware

Crypto ransomware is one of the most common flavors of ransomware. It encrypts a victim's files until a ransom is paid. This type of attack does not block full system access but rather targets specific datasets of value (or software applications in some cases). In many situations, the attacker will threaten complete data deletion if the ransom is not met. Some notable examples include: WannaCry, which exploited a previously unknown Windows vulnerability in 2017 and impacted over 200,000 global users, and CryptoLocker, which surfaced in 2013 and spread through the sharing of malicious email attachments.

CryptoLocker is considered by many to be the grandfather of modern ransomware as it was one of the first wide-spread examples to demand payment in the form of Bitcoin.

2. Locker Ransomware

Unlike crypto ransomware, locker ransomware locks users out of their entire operating system. This type of attack prominently displays large system-blocking ransom notes on the screen, preventing access to the desktop, files, and applications. Two notorious examples of locker ransomware include WinLocker and Police Locker ransomware. WinLocker famously utilized fake warnings which

claimed to have identified the presence of illegal activity on a victim's computer to manipulate them into paying a fine. Along a similar vein, Police Locker involved the impersonation of law enforcement agencies, falsely accusing victims of crimes and demanding payment to unlock the systems.

3. Ransomware-as-a-Service (RaaS)

It might seem hard to believe, but in a world where business reigns supreme, ransomware, too, has blossomed into a booming enterprise. RaaS is a business model in which ransomware developers sell or lease their malware to cybercriminals who then execute the code on victim machines. This framework is particularly troubling since it has enabled non-technical bad actors to rapidly implement malicious software without needing specialized skillsets. This evolution has ultimately led to a meteoric rise in ransomware groups such as REvil – a notorious ransomware 'gang' that operated between 2019 and 2021 targeting high-profile organizations and demanding multimillion-dollar ransoms.

4. Double Extortion Ransomware

Double extortion ransomware not only encrypts data but also threatens to publish stolen information unless a ransom is paid. This tactic pressures victims (especially those handling sensitive or classified data) into forced compliance. Maze, (a popular double extortion model) and Ragnar (which targeted large enterprises for maximum impact) are two prime examples of the risks associated with double extortion ransomware models.

5. Mobile Ransomware

The final notable class of ransomware is mobile ransomware which, as the name implies, targets smartphones, tablets, and mobile technology platforms. This ransomware often spreads through malicious apps or phishing links and either locks users out of their devices completely or encrypts specific files/folders. Fusob is a common example of mobile ransomware which targets Android devices and utilizes fake FBI warnings to try to trick users. Fusob operated similarly to Police Locker in that it exploits the "authority" social engineering tactic.

In summation, there are an immeasurable number of ransomware tactics, styles, and implementations, but the core tenets of ransomware remain the same: lock a system and demand a payment.

Insurance Considerations

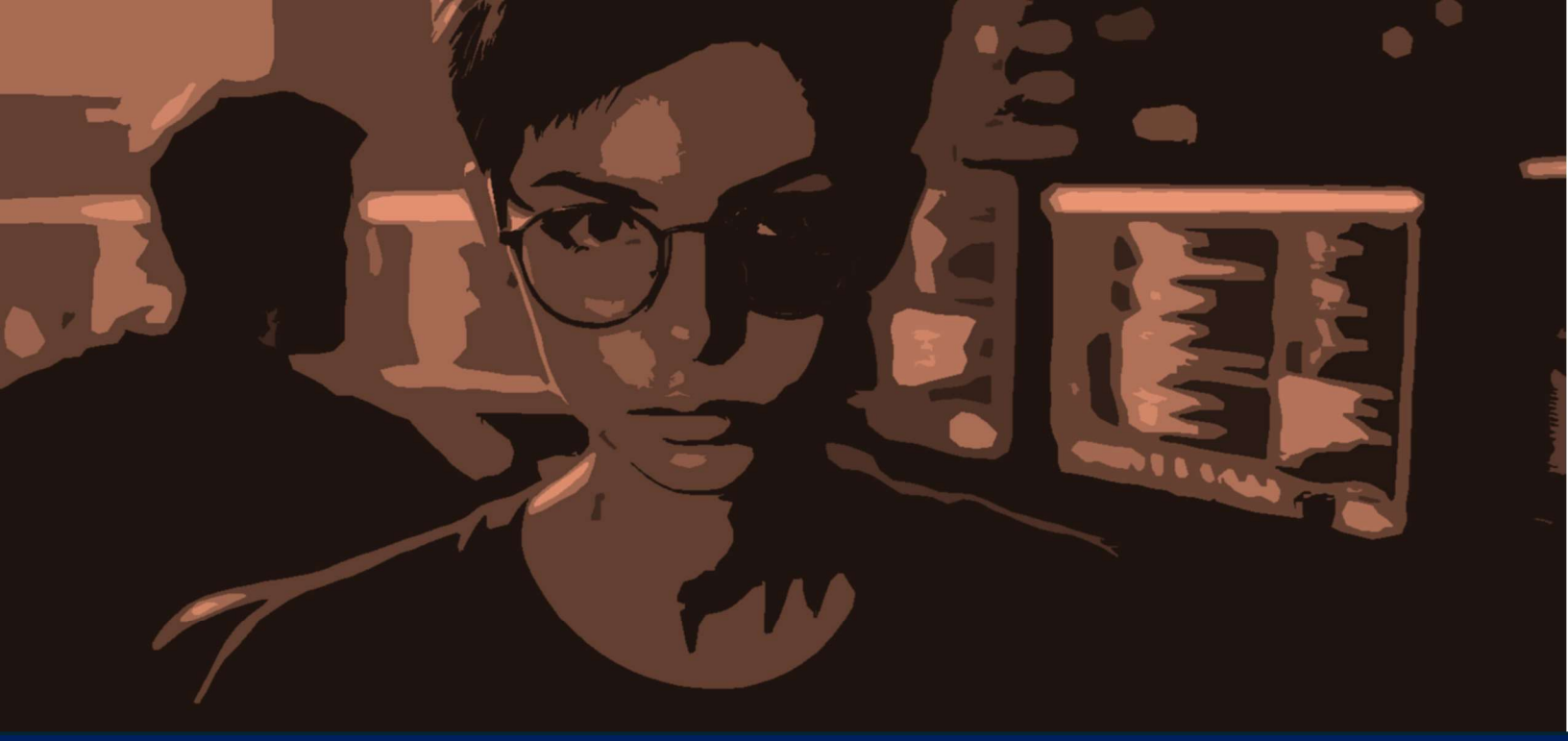
Many cybersecurity liability insurance providers will recognize ransomware as a notable event and categorize it as a 'peril' that falls under the umbrella of cyber coverage; thus, providing a certain level of financial support. What may not be common knowledge however is that financial support is not the only type of help that these insurance providers offer. Reputable providers also offer a variety of substantive support tools and access to professionals who can assist with recovery.

It is worth noting that some cybersecurity insurance providers offer independent guidance and stipulations regarding ransomware response and mitigations. As such, it is good practice to confirm what these requirements are prior to taking any internal actions towards ransomware abatement; as to avoid any violations. Cyber insurance policies often have specific requirements for incident response, including the use of pre-approved vendors for forensic investigation, legal representation stipulations, and pre-vetted negotiation strategies. Acting without insurer approval could result in degraded/limited coverage, the denial of claims, or even legal ramifications.

Many insurers also provide detailed guidance on best practices that align with regulatory requirements, depending on the industry enclave in which a given company operates in. For instance, an organization operating in the defense sector will have drastically different accepted ransomware abatement strategies than an organization operating in the healthcare sector. Similarly, some high-end cyber liability policies also include access to specialized teams of cybersecurity experts, such as incident response teams (IRTs), legal advisors, and business consultants who can help assess the *regulatory* impacts of attacks and determine courses of action.

Finally, insurers may have strict reporting and documentation requirements that must be followed to receive financial reimbursement for capital losses. Failure to adhere to these requirements, such as not reporting the incident within a specific timeframe or attempting to resolve the attack independently, could void coverage[5]. By involving the insurer from the beginning, organizations can ensure that all response efforts align with policy conditions and reduce potential liability.

[5]Insurance Training Center, "Asking the Right Questions – Ransomware and Insurance Edition"



Ransomware Roles and Responsibilities

Clearly defined roles and responsibilities during an incident (of any severity) are essential for ensuring a swift, coordinated, and effective response, and this theory holds true for ransomware response as well. Not only are uncoordinated response efforts ineffective, but they can often exacerbate the severity and impact of the event.[6] By establishing a structured response framework, organizations can ensure that all team members understand their duties, reducing downtime, and maintaining regulatory compliance. This proactive approach also improves decision-making, as key personnel will be prepared to act without hesitation when an incident occurs.

A well-defined incident response team also enhances accountability, ensuring that all aspects of the response are properly managed and documented. When roles are unclear, critical tasks such as evidence collection, threat containment, or communication with stakeholders may be overlooked. Additionally, defining roles in advance allows organizations to train personnel effectively, conduct simulations, and ensure that response protocols align with industry's best practices and cyber insurance requirements. Ultimately, role clarity strengthens an organization's overall security posture, making it more resilient to cyber threats.

[6]KPMG, "10 Common Cyber Incident Response Mistakes", Cyber Insights for the Federal Government

Common Roles

Incident Response Coordinator

Oversees the entire incident response process, ensuring that the response plan is executed effectively. This person acts as the main point of contact between technical teams, executives, and external stakeholders, such as law enforcement or insurance providers.

Technical Lead / Security Analyst

Responsible for investigating the attack, identifying vulnerabilities, and implementing containment measures. This role includes analyzing malware, reviewing system logs, and determining the scope of the breach.

Legal and Compliance Advisor

Ensures that the organization adheres to legal and regulatory requirements during the response. This includes advising on data breach notification laws, potential liabilities, and interactions with law enforcement.

Communications/PR Specialist

Manages internal and external communications, ensuring that employees, customers, and the media receive accurate and timely information. This role is critical for maintaining the organization's reputation and preventing misinformation.

IT / Infrastructure Lead
Works on restoring affected systems, applying patches, and strengthening security measures post-incident. This role ensures business continuity by coordinating with the technical team to recover data and services. This role is often filled by an external sub-contractor for smaller organizations, but may reside in-house for larger, more well-funded organizations.

Executive (CISO/CEO) Provides leadership and high-level decision-making, approving major actions such as ransom payments (if legally permissible) and allocating necessary resources for the response effort.

By clearly defining these roles and responsibilities, organizations can respond more efficiently to cyber incidents, minimize disruptions, and ensure compliance with legal and insurance requirements.

Having dedicated response personnel for ransomware incidents ensures rapid containment, minimizes damage, and enables a swift recovery, reducing downtime and financial loss.

Reporting Ransomware

Prompt reporting of ransomware incidents is crucial for mitigating damage, assisting law enforcement, and protecting others from similar attacks. Reporting procedures vary across industries, but several key agencies and organizations provide avenues for reporting ransomware attacks.

General Reporting

For most organizations and individuals in the United States, ransomware incidents should be reported to the following entities:

- **FBI Internet Crime Complaint Center (IC3):** The FBI investigates cybercrimes, including ransomware. Victims can file a complaint at https://www.ic3.gov.
- **Cybersecurity and Infrastructure Security Agency (CISA):** CISA provides support and resources to organizations dealing with cyber incidents. Reports can be submitted at https://us-cert.cisa.gov/report.
- **Federal Trade Commission (FTC):** The FTC tracks cybercrimes affecting consumers and businesses. Reports can be filed at https://reportfraud.ftc.gov.

Industry-Specific Reporting

Different industries may have additional reporting requirements due to regulatory and compliance obligations:

- **Healthcare (HIPAA-Regulated Entities):** Healthcare organizations must report ransomware incidents involving protected health information to the U.S. Department of Health & Human Services (HHS) Office for Civil Rights. Reports can be filed at https://www.hhs.gov/ocr.
- **Financial Sector:** Financial institutions must report cyber incidents, including ransomware, to the Treasury Department's Financial Crimes Enforcement Network (FinCEN) and their primary federal regulator. Reports can be submitted at https://www.fincen.gov.
- **Critical Infrastructure and Government Entities:** Operators of critical infrastructure, such as energy, transportation, and public services, should report incidents to CISA and the Department of Homeland Security (DHS) through https://us-cert.cisa.gov/report.

Paying the Ransom

In some rare cases, ransomware attacks against organizations with sub-par security protocols could directly impact critical files that are irreplaceable and for which there are no backups or alternative means of recovery available. In these cases, paying the ransom may be the only way to restore operations effectively, however, this decision should not be taken lightly and must be accompanied by extreme caution to minimize risk and avoid further exploitation.

Justifications for Paying the Ransom

Organizations facing a ransomware attack must weigh the risks and *potential* benefits of paying and must determine what the value of their systems and data ultimately are. Employing both qualitative and quantitative assessments, the organization needs to determine whether the possibility of getting their data back is worth the overall cost – an incredibly difficult decision to make. In an ideal world, all businesses would have robust backup solutions and recovery protocols in place to avoid this overwhelmingly negative scenario, however, in cases where backups are unavailable, outdated, or compromised, paying the ransom may be the only logical path to effective business restoration. It is not unrealistic to imagine situations where looming financial and reputational damage caused by prolonged downtime may outweigh the cost of the ransom itself.

Critical Infrastructure

Furthermore, critical infrastructure organizations, such as hospitals, defense agencies, and public utilities, may be unable to properly function without immediate access to encrypted data. In these extreme cases, paying the ransom is likely the only way to prevent severe consequences such as the loss of life or significant disruption of essential services. Although there is no guarantee that attackers will provide the correct decryption key following payment, many ransomware groups operate with a certain level of 'reliability' to maintain their reputation and encourage future victims to pay. Ransomware is a business after all, and if victims have a reasonable assurance that attackers will release their systems after rendering payment, then they will be far more likely to open their wallets following an event.

SRSLY, WTF?

Some ransomware hacker groups actually have "customer support" personnel that will help answer victims' questions and assist with processing ransom payments…

How nice of them.

Best Practices for Paying the Ransom

If an organization determines that paying a ransom is unavoidable, it should follow some basic best practices to reduce risk and avoid being further exploited:

Engage Cybersecurity Experts: Consult with cybersecurity professionals or a certified incident response team to assess the legitimacy of the attack and explore any alternative decryption methods before committing payment.

Negotiate the Ransom Amount: Some ransomware groups may be open to negotiation, potentially lowering the final payment amount. A professional ransomware negotiator can assist greatly in this process.

Verify the Attacker's Credibility: Research whether the ransomware group has a history of providing working decryption keys upon payment. Some groups have been known to take the ransom without delivering on their promise.

Use a Secure Payment Method: Most ransom demands require payment in cryptocurrency (typically Bitcoin or Monero). Organizations should ensure they follow proper procedures to maintain anonymity and comply with any legal obligations regarding cryptocurrency transactions.

Ensure Compliance with Legal and Regulatory Requirements: Paying a ransom may be illegal in some jurisdictions, especially if the attackers are affiliated with sanctioned or foreign entities. Consulting legal experts can help avoid inadvertent legal violations.

Document Entire Process: Keeping detailed records of communications, transactions, and decisions made throughout the incident can be useful for law enforcement investigations and future cybersecurity improvements.

Strengthen Future Security Measures: Regardless of the outcome, organizations should immediately bolster their cybersecurity defenses, including implementing stronger backup strategies, employee training, and endpoint detection and response (EDR) solutions.

While paying a ransom should always be a last resort, there are circumstances where it may be the only option to regain access to critical data. If payment is deemed necessary, following these best practices can reduce the risk of further exploitation.

The Importance of Documentation

In the face of a ransomware attack, proper documentation, chain of evidence, communications logs, and chronological event tracking are critical components of an effective response strategy. These elements ensure a structured approach to mitigating the attack, identifying the root cause, and facilitating recovery while preserving legal and regulatory compliance.

1. Documentation: Comprehensive documentation of the attack timeline, affected systems, and mitigation steps taken are essential for both immediate response and long-term security improvements. Proper records enable security teams to analyze attack patterns, refine defense mechanisms, and improve incident response protocols. Additionally, documentation supports compliance with industry regulations such as GDPR, HIPAA, and NIST standards, which often require detailed reporting of cybersecurity incidents.

2. Chain of Evidence (CoE): Maintaining a clear chain of evidence is also crucial for ransomware response, specifically for forensic investigations and taking potential legal actions against perpetrators. CoE ensures that all collected data, including logs, affected files, and attacker communications, remain unaltered and verifiable. Additionally, properly handling digital evidence can aid law enforcement in possibly identifying threat actors and may contribute to legal proceedings against these cybercriminals. Organizations should follow established forensic best practices to maintain evidence integrity and admissibility in court.

3. Communications Logs: Tracking all communications during a ransomware incident is vital to understanding how the attack unfolded and ensuring accurate information dissemination. Logs of internal and external communications help prevent misinformation, coordinate incident response efforts, and provide an auditable record for post-incident review. This documentation is also critical for managing public relations, ensuring transparency with stakeholders, and maintaining trust with customers and partners. This documentation should be centralized within an organization and should be available to all key stakeholders.

4. Chronological Event Tracking: A detailed timeline of events, including the initial infection, detection, containment, involved parties, remediation steps, etc. provides clarity on attack progression and response effectiveness. This information will ultimately help the security team(s) identify gaps in their defenses, improve response times, and develop better-preparedness strategies for future incidents. Additionally, chronological tracking is essential for filing insurance claims and reporting to regulatory agencies. Proper chronological log tracking ("ChronoLogging") demonstrates due diligence in incident handling procedures.

   Although meticulous documentation during emergency response activities may seem like a misallocation of resources (at the time), it is paramount to ensure that key details and elements of the investigative activities are captured and verified. Documentation is one of the most important aspects of professional incident response and ransomware mitigation.

Ransomware Phases

A wholistic approach to ransomware preparedness and response can be broken into five core event phases: Prevention, Training, Detection, Response, and Recovery; and each requires a tailored and deliberate level of attention. Since little can be done *following* a ransomware attack, many of the recommended mitigation strategies and control adjudications for ransomware events occur *prior* to the attack, however there are some notable action items that can be (and need to be) conducted during and after an event as well. These 5 phases are the basis of the SecurityInsecurity Ransomware Preparedness & Response Checklist and can drastically reduce system downtime, expediate remediation activities, and assist with executive-level decision making throughout a ransomware event.

Checklist Usage

The following checklist is designed to be a supplement to a robust and fine-tuned cybersecurity management framework and should not be used as a sole-source ransomware response strategy. When implemented correctly, this checklist can provide organizations with an actionable approach to preparing for and handling a ransomware event efficiently.

Preparedness & Response Checklist

Prevention

Regular Backups

- Maintain frequent offline and cloud-based backups.
- Test backups regularly to ensure they are recoverable.

Endpoint Protection & Security

- Deploy antivirus and endpoint detection and response (EDR) solutions.
- Enable automatic updates for security patches.

Network Security

- Segment networks to prevent lateral movement.
- Implement strong firewall and intrusion detection/prevention systems.

Access Controls

- Enforce multi-factor authentication (MFA)
- Use the principle of least privilege for access

Email and Web Security

- Implement email filtering for phishing detection.
- Educate employees about suspicious links and attachments.

Software & System Updates

- Apply security patches promptly to all systems
- Disable unnecessary services and software.

Incident Response Plan

- Develop and document a ransomware-specific response plan.
- Train employees in their roles and responsibilities following an incident.

Training

Employee Training Programs

- Conduct regular cybersecurity training sessions.
- Provide interactive workshops on identifying phishing and ransomware threats.

Simulated Attacks

- Run periodic ransomware simulation exercises to test response capabilities.
- Analyze simulation results and adjust training accordingly.

Role-Based Training

- Offer specialized training for IT and security teams on incident response.
- Ensure executives and decision-makers understand their role in a ransomware event.

Detection

Log and Event Monitoring

- Enable logging for system and security events.
- Use security software for real-time detection.

User Behavior Analytics

- Monitor for abnormal behavior, such as mass file encryption or unauthorized access attempts.

Threat Intelligence

- Stay updated on emerging ransomware threats and attack vectors.

Response

Incident Response Team (IRT)

- Identify key personnel and their roles in an attack scenario.
- Establish clear communication channels and an escalation plan.

Coordinate with a Professional Consultancy Agency

- It is best practice to contract a professional cybersecurity firm to coordinate ransomware response activities.

Containment Strategies

- Have playbooks for isolating infected systems.
- Disable affected accounts and limit access.

Legal & Compliance Considerations

- Understand regulatory obligations for reporting ransomware incidents.
- Establish contacts with law enforcement and cybersecurity firms.

Recovery

Restore From Backups

- Verify integrity before restoring to avoid reinfection.
- Ensure recovery time objectives (RTOs) align with business needs.

Post-Incident Analysis

- Conduct a forensic investigation to determine root cause.
- Update security policies and procedures based on lessons learned.

Employee Awareness and Training

- Conduct regular security awareness training.
- Simulate phishing and ransomware attacks to test preparedness.

Final Check: Ensure leadership, IT, and security teams review and approve this checklist periodically to keep it up to date.

Ransomware Response Timeline

Pre-Incident

- Implement a robust security program & conduct simulation events
- Develop an Incident Response Plan (IRP) & gain management buy-in
- Generate regular system backups & frequently test recovery steps
- Segment network clusters & engage in offensive security

T=0 Detection

- Confirm the presence of an attack& begin initial data collection
- Alert Incident Response Team (IRT) & start containment efforts
- Assess the scope of the incident & execute the IRP

T= 1-6 Hours

- Begin detailed evidence collection & chrological log documentation
- Determine attack vector and event impact (forensics)
- Notify key stakeholders, customers, clients, and vendors (as needed)
- Engage with the legal department/legal representation

T+6-24 Hours

- Digitally isolate the affected systems & scan tangential clusters
- Verify backup availability and integrity
- Engage law enforcement (if needed) and begin reporting to regulatory agencies
- Develop a strategy/stance on payment (worst-case scenario)

T+24-72 Hours

- Begin system restoration with verified backups (if available)
- Patch exploited vulnerabilities on impacted system and tangential clusters
- Place staff on high alert for repeat attacks & scan for additional weaknesses
- Conduct internal investigations, assess the possibility of insider threat, etc.

T+3-7 Days

- Conduct root cause analysis & document findings
- Enhance security measures according to weaknesses identified
- Re-train employees & verify the efficacy of response procedures
- Report findings, conduct lessons learned & close out the event

When in doubt, contract with trusted professionals on ALL ransomware activities.

DON'T GO IT ALONE

SECURITY IN SECURITY

Partner with SecurityInsecurity today.

Ask about our flexible pricing.

www.securityinsecurity.com

978-480-0890

Partnering w/ SecurityInsecurity

Your Cyber and Compliance Provider

Proactive Ransomware Preparedness

At SecurityInsecurity, we believe in stopping cyberattacks *before* they happen through a holistic approach including:

- ✓ Risk Assessments
- ✓ Advanced Threat Detection
- ✓ Backup & Disaster Recovery
- ✓ Employee Training & Phishing Defense
- ✓ Incident Response Planning

Comprehensive Cybersecurity Support

SecurityInsecurity provides **end-to-end** protection designed for growing businesses. We despise the *one-size-fits-all* approach to cybersecurity and we believe that cyber software should be used as a tool, not as a sole-source solution. Your organization is unique, your approach to cybersecurity should be as well.

- ✓ Security Monitoring
- ✓ Cloud & Endpoint Security
- ✓ Compliance & Regulatory Support
- ✓ Cost-Effective, Scalable Solutions

Why SecurityInsecurity?

- ✓ Expertise You Can Trust
- ✓ Fast Response, Minimal Downtime
- ✓ Customized Approach
- ✓ Proactive, Not Reactive
- ✓ **Lowest Prices in the Industry!**

Ransomware Preparedness and Cybersecurity

SecurityInsecurity is an American-owned and operated technology company that specializes in cybersecurity & compliance support for small and medium-sized businesses (SMBs) and emerging enterprises, alike. Our team focuses on maximizing organizations' existing cybersecurity infrastructures, without spending unnecessary time or resources on bloviated hardware/software "solutions". Whether you need top-tier ransomware preparedness or comprehensive cybersecurity support tailored to your unique challenges, SecurityInsecurity is the trusted partner for you.

P.O. Box 1353
East Northport, NY 11731
(978) 480-0890
cyber@securityinsecurity.com
www.securityinsecurity.com

SECURITYIN SECURITY

Index

Additional References

January 22, 2024. University of Tulsa. "Famous Ransomware Attacks in History". https://online.utulsa.edu/blog/famous-ransomware-attacks-in-history/
National Cyber Security Centre. "A Guide to Ransomware". https://www.ncsc.gov.uk/ransomware/home
October 5, 2021. CSR. "Ransomware and Federal Law: Cybercrime and Cybersecurity". https://www.congress.gov/crs-product/R46932
March 01, 2022. Cybersecurity & Infrastructure Security Agency (CISA). "Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)". https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

Legal Disclaimer

The information contained in this guidebook is provided for educational and informational purposes only. It is not intended to serve as the primary source of information for incident response or as a substitute for professional cybersecurity advice, training, or consultation. While every effort has been made to ensure the accuracy and reliability of the content, SecurityInsecurity makes no guarantees, express or implied, regarding the completeness, suitability, or applicability of the information presented.

SecurityInsecurity shall not be held liable for any damages, losses, or consequences resulting from the use or misuse of the material contained in this guidebook. Organizations and individuals are encouraged to consult with qualified cybersecurity professionals and follow industry best practices when responding to security incidents.

For any questions, comments, or concerns regarding the material produced, SecurityInsecurity is available to provide further clarification and support.

Author: William Spettmann
President, SecurityInsecurity
M.S. Cybersecurity & IT Management
CISSP, PMP, CISM, C|EH, C|NDA, Security+

Co-Authors: Max Spettmann
Director of Cybersecurity
Security+, HITRUST

Nicole Carron
Director of Cyber Governance

Editor: Alexandra (Riccardi) Spettmann
Director of Business Development

Tech Editor Christopher R. Sanchez
Director of Information Technology