Active Cyber Defense

Ransomware: Fast Facts

An Infographic

KONICA MINOLTA

Defining Ransomware

- Ransomware is a type of malicious software cyber actors use to deny access to systems or data.
- The malicious cyber actor holds systems or data hostage until the ransom is paid.
- After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems.
- If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

Source: U.S. Department of Homeland Security

FBI on Ransomware

High-impact Ransomware Attacks Threaten U.S. Businesses and Organizations

- The FBI estimates that ransomware infects more than **100,000** computers a day around the world and ransom payments approach **$1 billion** annually. Unfortunately, these numbers are only expected to rise in the future.
- Ransom payments, however, do not account for all of the costs associated with a ransomware attack. Unrecoverable data, lost productivity, damage to reputation, damaged equipment, forensic investigations, remediation expenses, and legal bills are some of the additional costs that can be expected when responding to a ransomware attack.
- The actual cost of a ransomware attack may be several times more than just the ransom paid. The U.S. Department of Justice called the use of ransomware a global phenomenon and a new business model for cybercrime.

High Risk

Source: Cybersecurity Ventures

Ransomware attack costs, **$6 Trillion by 2021.**

Ransomware: How Does the Attack Work?

Ransomware starts with an unsolicated email, typically designed to trick the victim into clicking on an attachment or visiting a webpage.

The ransomware leverages flaws in the computer's operating system to force it to run ransomware code.

The ransomware encrypts important files on the system and demands a ransom payment using the digital currency bitcoin.

High Risk

Phishing

In 2020, ransomware from phishing emails increased **109 percent**. Phishing emails are a common delivery vehicle for ransomware.

High Risk

Ransomware Facts

A new organization will fall victim to ransomware **every 11 seconds in 2021.**

ecfirst | CMMC|NIST ecfirst Academy | CCSA Certified Cyber Security Architect

Cyber Resilience In the 2020s

Global Cybersecurity & Compliance Expert

Code: RANSOMNHW0023

Active Cyber Defense

Ransomware: Fast Facts

An Infographic

KONICA MINOLTA

Seven Action Steps to Address if Infected with Ransomware

1. Isolate the infected computer immediately.
2. Isolate or power-off affected devices that have not yet been completely corrupted.
3. Immediately secure backup data or systems by taking them offline.
4. Contact law enforcement immediately. (Eg. FBI).
5. If available, collect and secure partial portions of the ransomed data that might exist.
6. If possible, change all online account passwords and network passwords after removing the system from the network.
7. Delete Registry values and files to stop the program from loading.

High Risk Ransomware Types

The top five ransomware variants argeting U.S. companies and individuals are:

- CryptoWall
- CTBLocker
- TeslaCrypt
- MSIL/Samas
- Locky

Protecting Your Business

Backups: Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?

Risk Analysis: Have we conducted a cybersecurity risk analysis of the organization?

Staff Training: Have we trained staff on cybersecurity best practices?

Vulnerability Patching: Have we implemented appropriate patching of known system vulnerabilities?

Application Whitelisting: Do we allow only approved programs to run on our networks?

Incident Response: Do we have an incident response plan and have we exercised it?

Business Continuity: Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?

Penetration Testing: Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

High Risk Software Vulnerabilities

Criminals plant ransomware on websites and take advantage of software vulnerabilities to launch attacks on visitors using outdated software (browser, browser plugin).

High Risk COVID-19 Ransomware

Businesses and end-users are being targeted to download COVID-19 ransomware disguised as legitimate applications.

ecfirst | CMMC|NIST ecfirst Academy | CCSA Certified Cyber Security Architect

Code: RANSOMNHW0023

Cyber Resilience In the 2020s

Global Cybersecurity & Compliance Expert

Active Cyber Defense

Ransomware: Fast Facts

An Infographic

KONICA MINOLTA

FBI Guidance on Ransomware Cyber Defense Best Practice

- Regularly backup data and verify its integrity.
- Focus on awareness and training.
- Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered.
- Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.
- Implement the least privilege for file, directory, and network share permissions.
- Disable macro scripts from Office files transmitted via email.
- Implement software restriction policies or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular internet browsers, and compression/decompression programs, including those located in the AppData/LocalAppData folder.
- Employ best practices for use of RDP, including auditing your network for systems using RDP, closing unused RDP ports, applying two-factor authentication wherever possible, and logging RDP login attempts.
- Implement application whitelisting.
- Use virtualized environments to execute operating system environments or specific programs.
- Categorize data based on organizational value, and implement physical and logical separation of networks and data for different organizational units.
- Require user interaction for end-user applications communicating with websites uncategorized by the network proxy or firewall.

Targeted Ransomware Attack

- A targeted ransomware attack is loosely defined as a ransomware attack that is adapted to a specific organization or industry. In such incidents, ransomware can be customized and deployed based on the size and sophistication of a potential victim, the sensitivity of data, and the malware code can be adjusted to be more effective in certain situations, for example, by exploiting specific vulnerabilities present in targeted systems. The ransom demands for this type of attack are often set according to the victim's percieived ability to pay.
- Cybercriminals soon found that customizing their attacks to specific, "quality" targets led to an increase in the amount of ransom payments.
- Organizations commonly targeted by this type of attack have sensitive data, high data availability requirements, low tolerance for system downtime, and the resources to pay a ransom.
- Many healthcare organizations fit this profile, and have become targets.

High Risk

Ransomware & COVID-19

March 2020, ransomware dubbed 'Covidlock' was spread disguised as a coronavirus tracking app.

Numerous attempts have been observed of delivering malicious payloads including those related to the COVID-19 theme.

High Risk

IBM, Inside the 2020 Report

- **8.5 billion** records breached in 2019, giving attackers access to more stolen credentials.
- **150,000** vulnerabilities disclosed to date.
- Ransomware attacks up **67%** year-over-year.
- North America is the biggest geographic target.

ecfirst | CMMC|NIST ecfirst Academy | CCSA Certified Cyber Security Architect

Code: RANSOMNHW0023

Cyber Resilience In the 2020s

Global Cybersecurity & Compliance Expert

Active Cyber Defense

Ransomware: Fast Facts

An Infographic

KONICA MINOLTA

Business Impact Analysis (BIA)

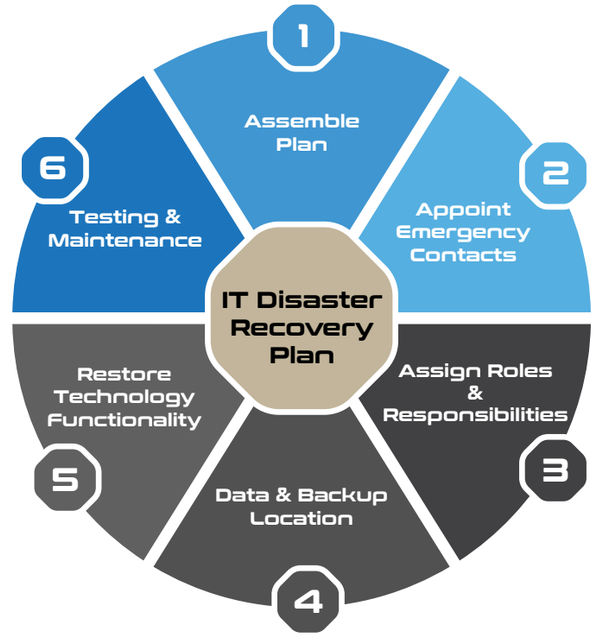
- Foundation for building Contingency Plans.
- Identify and prioritize critical IT systems, applications and components.
- Two types of Contingency Plans
  - Emergency Mode Operations Plan for business unit recovery.
  - IT Disaster Recovery Plan (IT DRP).
- The BIA must establish:
  - Tolerance for disrupted business processes, including human impact (e.g. pandemic).
  - Identification of exposures to continuous availability of services and key personnel (IT and others).
  - Possible mitigation strategies.
  - Application priorities and availability requirements.
  - Anticipated disruption impact on department operations.
  - Departmental processing priorities and availability requirements.

Project Goal for a BIA

- Examination of specific compliance requirements that must be met – focus on security, business continuity, and disaster recovery.
- Identification of risks to interruption of service.
- Business continuity/disaster recovery solutions that are appropriate to business impact and result in a comprehensive BIA Report.
- Identification of critical activities to be able to appropriately respond to service disruptions or disasters.

IT Disaster Recovery Plan (DRP)

- Objective is to establish procedures to restore any loss of data (patient data is a critical asset).
- Applies to major, usually catastrophic, events.
- Ability to quickly handle incidents can reduce downtime and minimize both financial and reputational damages.
- DRPs allow organizations to ensure they meet all compliance requirements, while also providing a clear roadmap to recovery.
- The BIA identifies the impacts of disruptive events (e.g. pandemic) and is the starting point for identifying risk within the context of disaster recovery.
- The RA identifies threats and vulnerabilities that could disrupt the operation of systems and processes highlighted in the BIA.



ecfirst | CMMC|NIST ecfirst Academy | CCSA Certified Cyber Security Architect

Cyber Resilience In the 2020s

Global Cybersecurity & Compliance Expert