ISACA

Blueprint for Ransomware Defense

Information Security

CONTENTS

ABSTRACT

Ransomware attacks continue to increase in frequency, complexity and damaging effects worldwide.[1] Cybercriminals have operationalized ransomware into a multibillion-dollar illegal enterprise with the capability to exploit and disrupt even the largest and most sophisticated companies. However, both the probability and severity of an attack can be mitigated when companies develop and maintain strategies for both prevention and mitigation. This white paper offers insight into the current ransomware landscape and outlines steps an organization can take to prepare for and respond to ransomware attacks.

1 Dorfman, Max; "Cyberattacks Growing in Frequency, Severity, and Complexity," The Triple-I Blog, Insurance Information Institute, 29 April 2022, http://www.iii.org/insuranceindustryblog/cyberattacks-growingin-frequency-severity-and-complexity/

Introduction

Ransomware is malware that threatens to permanently restrict access to a system or publish compromised data if a ransom demand is not satisfied. Once a system is compromised, data are then encrypted, and access is blocked until payment is received in exchange for the promise of decryption keys.

Cybercriminals have operationalized ransomware into a multibillion-dollar criminal pursuit, with the capability to exploit and disrupt even the largest and most sophisticated companies. A ransomware attack can, at best, temporarily impact revenue generation, or at worst, cause a massive financial loss that triggers bankruptcy or liquidation.

Anecdotal evidence suggests that far too many organizations across both private and public sectors lack basic cybersecurity practices therefore keeping the cost of business affordable for bad actors. This in turn has resulted in varied degrees of governmental response, often in the form of legislative action.

Given the reach of governmental mandates, public entities have less flexibility to address potential ransomware threats and responses (at least for the foreseeable future), while private enterprises still possess the ability to decide whether to pay ransom. Whether to pay ransom is heavily debated and outside the scope of this white paper.

Given the diverse and invasive nature of information technology, the variety of controls that must be implemented, and the varied level of integration of those controls into operations, an effective defense in one environment may not work in another. The control risk has a range of root causes, from the misinterpretation of a new business control requirement and its intent to improperly trained staff. In addition, each attack is unique because motivations and objectives often require the adversary to remain nimble and adapt, unhindered by enterprise defense.

Enterprise culture is also one of the strongest influences on its ability to prepare, defend and recover from an attack. Depending on the enterprise maturity, this can mean the difference between actual preparedness or a false sense of security.

Enterprise culture is one of the strongest influences on the enterprise's ability to prepare, defend and recover from an attack. Depending on the enterprise maturity, this can mean the difference between actual preparedness or a false sense of security.

This white paper provides information about ransomware attacks and presents detailed guidance on how to prepare for and respond to them. Cybersecurity, while challenging, is highly influenced by variables which include but are not limited to business size, sector and industry.

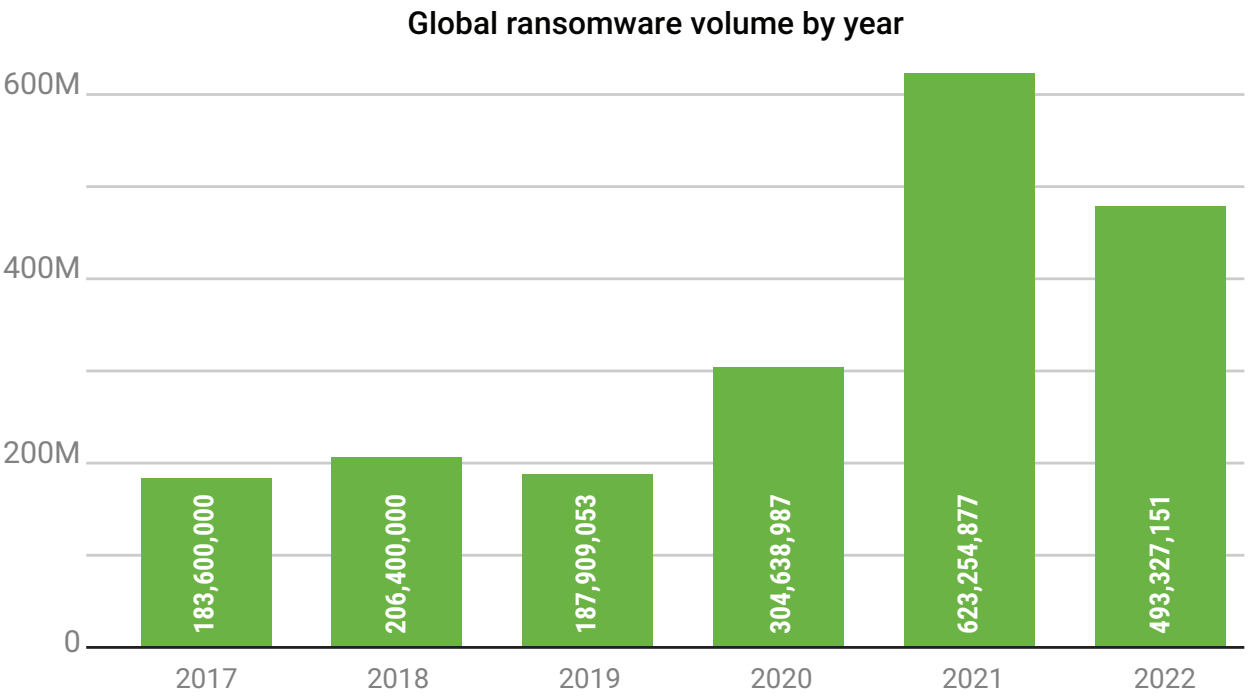
The Rise of Ransomware

Although ransomware attacks have been interrupting business operations since 1989, the number of such attacks is rapidly increasing. The Verizon *2022 Data Breach Investigation Report* reveals a "13% increase in ransomware breaches—more than in the last 5 years combined."[2] **Figure 1** shows the worldwide rise of ransomware from 2017 to 2022.

2 Verizon Business Resources, "2022 Data Breach Investigations Report," 2022, http://www.verizon.com/business/resources/reports/dbir/

Cybercriminal groups continue to evolve their operations and grow their marketspace. **Figure 2** shows a cost-benefit analysis of running a simple commodity ransomware campaign. The result shows the low barrier to entry into ransomware.

FIGURE 1: Global Ransomware Volume by Year



Source: SonicWall, Inc., "2023 SonicWall Cyberthreat Report," 2023, https://www.sonicwall.com/2023-cyber-threat-report/

FIGURE 2: Cost-Benefit Analysis of Ransomware Campaign

It's simple math!

Cost to develop ransomware
- 160 hours at $200/hour

Cost of disposable infrastructure
- 10 servers at $500 ($50/server)

Cost of launching ransomware attack
- Push "button" to start
- Monitor for 10 days (240 hours at $150/hour)

Attack 1,000,000 targets
- 1% pay the ransom at $300/system

	Cost
Developer	$32,000
Infrastructure	$500
Launch attack	$50
Help desk	$36,000
Investments	$68,550
1% target market share	$3,000,000
Return on investment	**$2,931,450**

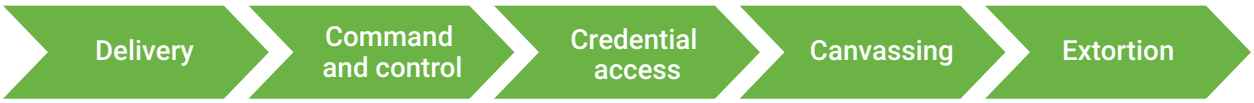
Source: Hinsch, Nicholas; "Louisville Metro ISSA Louisville, KY 2019–Ransomware Recovery," 18 November 2019, http://www.therubiconadvisorygroup.com/2019/11/18/louisville-metro-issa-2019/

Ransomware Life Cycle

As cybersecurity practices evolve to keep up with changing digital landscape, bad actors continue to change and adapt to overcome those practices. A simple web query will net countless variations of a ransomware attack life cycle. For instance, one prominent financial entity published insights visualized in **figure 3**.

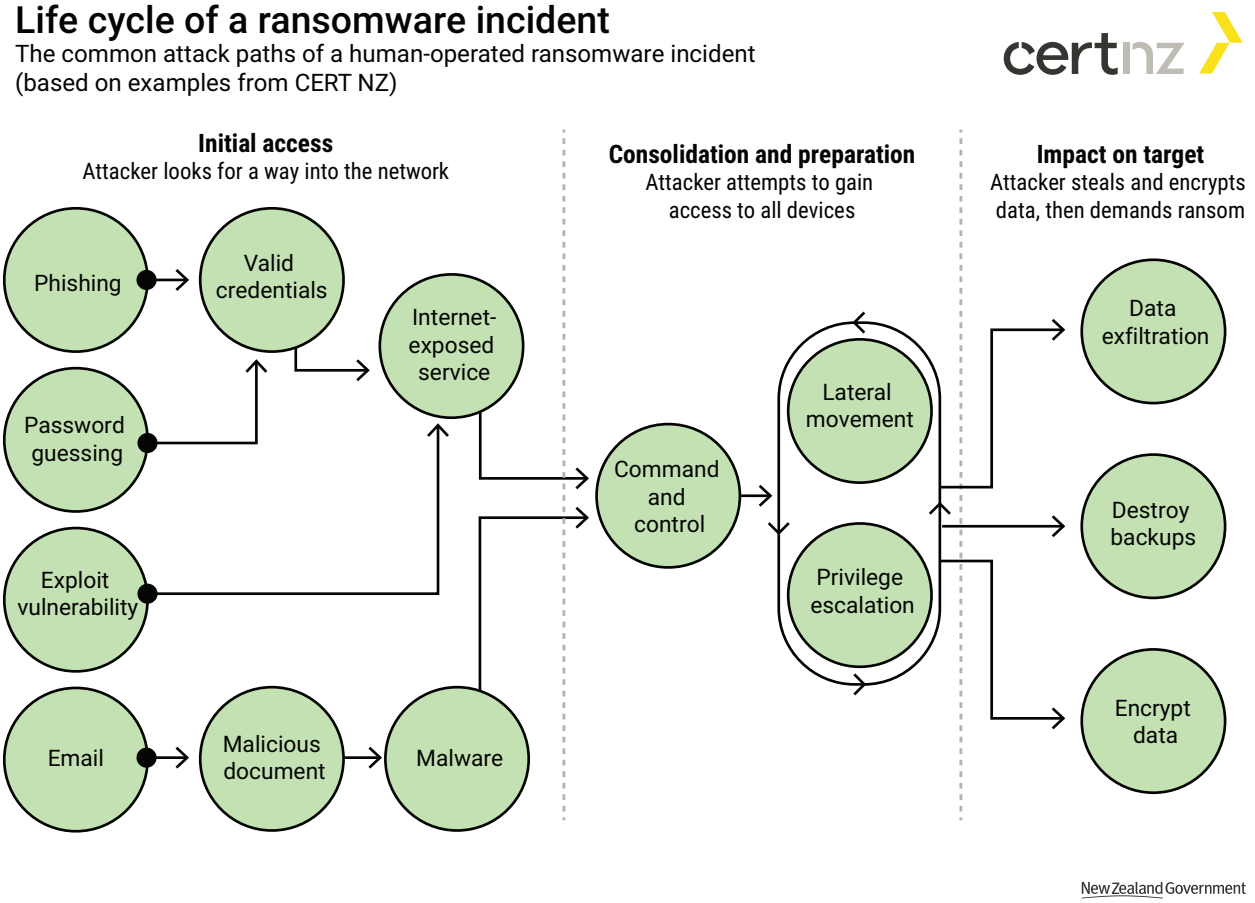
A more detailed life cycle from the New Zealand CERT is shown in **figure 4**.

FIGURE 3: Five Stages of a Ransomware Attack



Source: JPMorgan, "The Anatomy of a Ransomware Attack," 7 September 2022, http://www.jpmorgan.com/commercial-banking/insights/the-anatomy-of-a-ransomware-attack

FIGURE 4: New Zealand CERT Life Cycle of a Ransomware Incident



Source: Government of New Zealand and CertNZ, "How Ransomware Happens and How to Stop it," http://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/ © Govt NZ 2023. Reprinted under https://creativecommons.org/licenses/by-nc/4.0/.

Understanding the life cycle of a ransomware attack can help business professionals identify threats, assess risks, and implement effective mitigation strategies. It also enables them to develop an incident-response plan and promote a culture of cybersecurity awareness.

Ransomware Incident Types

We have seen malicious software evolve from manual computer to computer transfer (e.g., floppy disk or USB drive) to virus replication to the development of remote access tools. Previously, organizations were attacked and their private information compromised with the intent that the stolen information would be sold within the criminal underground. Now, criminals weaponize cryptographic software or use system encryption functionality. They demand immediate payments via cryptocurrency. Our readiness and ultimate response to these threats must change. Ransomware is no longer for amusement but rather has become a highly lucrative business.

Ransomware is no longer for amusement but rather has become a highly lucrative business.

The three major ransomware incident types are:

- **Mass Automated Infection of Isolated Systems**—Threat actors cast very wide nets and are heavily reliant on automation to exploit and spread ransomware to targets of opportunity. Typically, these yield a lower return on investment to the threat actor. This attack type was common between 2015–2019 before the emergence of the enterprise ransomware.
- **Enterprise Ransomware (aka "Big Game Hunter")**—Threat actors focus on targeted intrusions for profit (extortion). The victims are usually enterprise networks of small to medium enterprises and large organizations. Enterprise ransomware constitutes the most common form of ransomware attack after 2019, and it is also responsible for most of the innovation around extortion tactics and the emergence of ransomware supply-chain ecosystems (i.e., access brokers, exchange and money mule services, bulletproof hosting, malware delivery networks, etc.)[3]
- **Ransomware-as-a-Service (RaaS)**—This is a novel delivery model designed to support enterprise ransomware operations in which ransomware developers lease/offer the malicious code to qualifying affiliates (aka "operators") who possess the hacking skills to execute targeted intrusions and deploy ransomware in enterprise networks. The model allows ransomware developers to reduce the skill level required to launch a ransomware attack and to scale up those attacks by offering up ransomware to multiple affiliates while also transferring to those affiliates the risk of getting identified and arrested. Affiliates receive the largest percentage of the ransom (usually around 60–70%) and don't have to manage the extortion activities (e.g., negotiations, cryptocurrency transfers, leak site management, ransomware development, etc.).

Ransomware Threat Actors

Three main types of threat actors generate ransomware attacks:

- **Criminal Groups**—The only objective of these threat actors is to make money. They view a ransomware attack as a business transaction in which currency is extorted from a target.
- **State-Sponsored Threat Actors**—These actors focus on disruption to further their geopolitical and sociopolitical goals and influence the direction of a target. State-sponsored actors are backed by their governments. Ransomware is often used in advance of a kinetic engagement, as seen with the Russo-Georgian War in 2008 and more recently with suspected Russian campaigns targeting Poland, disrupting transportation and logistics organizations and a key conduit supplying military aid to Ukraine.[4]
- **Ransomware-as-a-Service (RaaS) Providers**—Threat actors use a criminalized version of Software-as-a-Service, in which ransomware campaign risk (e.g., costs, resources and legal) is reduced and returns are shared between affiliate members and the RaaS provider.

Current Observed Ransomware Trends

Threat actors are refining their operations—Instead of investing resources to gain access, threat groups are leveraging their relationships with initial access brokers, allowing the threat groups to spend more time orchestrating targeted attacks instead of investing

3 theNET By CLOUDFLARE, "Ransomware attackers escalate extortion tactics," http://www.cloudflare.com/learning/insights-ransomware-extortion/
4 Cybersecurity & Infrastructure Security Agency (CISA), "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." Retrieved 2 March 2023. http://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

resources to initially compromise a target. This also opens the market to less sophisticated attackers who may not have the experience, skill or capability to breach perimeter defenses, but can follow a runbook.

Changes in threat-group operations require enterprises to review their security awareness and training programs and ensure that their workforces are well aware of both the ransomware threat and their company's ransomware policies. An employee's policy-awareness should include the official company stance and response, e.g., "Acme will never pay a ransom" vs. "Acme will approach ransomware on a case-by-case basis."

Changes in threat-group operations require enterprises to review their security awareness and training programs and ensure that their workforces are well aware of both the ransomware threat and their company's ransomware policies.

Because enterprises must transform, adapt and innovate to maintain a dominant presence in the marketspace, criminal operators must do the same. Threat actors are investing in their products to adapt to the changing market landscape, i.e., the enterprise attack surface.

Threat groups are specializing and maturing their technical capabilities, often faster than enterprises can learn to adapt and defend against them. This rapid rate of innovation and adaptation requires enterprises to continuously monitor for threats and to enhance their incident-management and digital-forensics (reverse engineering) capabilities.

Ransomware barrier to entry is dropping—The landscape of cyberattacks has evolved significantly, with the advent of Ransomware-as-a-Service (RaaS) which allows malicious actors to leverage pay-for-use malware to launch and sustain ransomware campaigns. Rather than having to develop their own ransomware code and execute a tailored set of operations, attackers can now avail themselves of a platform that offers the requisite ransomware code and operational infrastructure. The increase in as-a-Service providers (e.g., initial access brokers and tailored ransomware packages) is decreasing the cost to enter the ransomware marketplace. The barrier to entry is at an all-time low, and it continues to drop, allowing more threat actors to enter the market.

This drop in cost is another driver for enterprises to look objectively at their plans and preparations for threat attacks.

Threat actors are getting better at hiding their identity and actions—Threat actors obscure their identities, leveraging common anonymizing services not only when they interact with their criminal counterparts, but also to make it more difficult for enterprises to defend against attacks. Attackers also use ethically flexible VPN and cloud-service providers to further obfuscate their origin.

Better identity obfuscation reinforces the need for enterprises to upgrade their threat-hunting and incident-management capabilities.

Zero-day exploits are rising—In the past, phishing campaigns have been the most successful method for adversaries to gain their foothold. Today, zero-day exploits are more common, from highly publicized remote exploits like Log4J (CVE 2021-45046), to a variety of Microsoft Windows-based exploits,[5] highlighting the need for inventory maintenance, configuration management, vulnerability management and patch management programs.

In addition to the data hygiene practices common to a businesscentric security management program, these exploits show the need for additional protection, e.g., attack-surface management, threat hunting, patch management, network segmentation and baselining behavior (network and user).

The use of artificial intelligence to create ransomware is emerging—Accessibility and ease of artificial intelligence (AI) allows it to be weaponized, further lowering the barrier to entry for ransomware. Although current AI can create basic and rudimentary ransomware capabilities that may not be sophisticated enough to bypass available endpoint detection and response (EDR), extended detection and response (XDR) or managed detection and response (MDR) platforms, the global

5 MS Office Graphics Remote Code Execution (CVE 2022-47213), MS Edge Elevation of Privileges (CVE 2022-44708), MS SharePoint Server Remove Code Execution (CVE 2022-44690).

rate of adoption of such platforms warns us that many businesses may find themselves victims of this type of attack.

As AI capabilities increase, more bad actors will leverage it, requiring all enterprise professionals to maintain a higher level of vigilance.

Double Extortion—A tactic employed by threat actors who, after encrypting a target's files, then exfiltrates and threatens to release those files. This was first employed in 2019 and has since increased the effectiveness of ransomware campaigns. While most ransomware attackers invest in breaching organizations (big game hunters), some threat actors are using Ransomware-as-a-Services who still leak data, even after ransom for the data has been paid.

Triple Extortion—A tactic used in which additional attacks (i.e., Distributed Denial of Service) are employed to apply additional pressure to targeted organizations.

Preparedness and Readiness

Ransomware, just like any other threat we face in business, requires a formalized preventative approach and protective stance. Just as organizations define and establish policies for ensuring the proper management of other business affairs, cybersecurity protocols need to be clear and concise, articulating the appropriate and expected response should your organization be attacked with ransomware.

The ransomware policy provides the rationale and justification about why investments are made in one area over another or why certain changes to business operations are made.

The good news is that by getting back to basics of systems and network hygiene, enterprises can address and mitigate many attacks. Implementation of egress filtering increases the likelihood of being able to interrupt communication with command and control (C2) nodes. Done correctly (and enforced), network segmentation actively reduces overprovisioned accounts. Lastly, backups must meet business needs and be tested for usability.

Governance

When a ransomware incident occurs, the response timer is counting down. Therefore enterprises should have a plan for their approach to the threat. An official ransomware policy informs and directs enterprise practices and operations, and its response to a ransomware incident.

Senior management needs to define their official stance on extortion attacks. The ransomware policy provides the rationale and justification about why investments are made in one area over another or why certain changes to business operations are made.

Ransomware/extortion does not necessarily need to be its own policy. What matters most is that ransomware attacks are adequately covered in crisis management, business continuity, incident detection and response playbooks, etc.

Figure 5 shows enterprise ransomware/extortion policy levels and the consequences of not having a policy.

FIGURE 5: Ransomware/Extortion Policy Levels

Levels of Ransomware/Extortion Policy		
We Will Not Pay	**Limited Basis**	**No Defined Policy**
• Under no circumstances will we pay a ransom. • This will require the Board and senior management to meet. This also will inform decisions and should be used to justify resource acquisition and investments. • This requires an intimate knowledge and understanding of the operating environment and justification and traceability for the investments in the people, processes and technology in IT-related business programs. The infrastructure needed to satisfy this requirement must reach the entirety of the organization. • This includes significant investments and dedication of resources into IT-related business programs.	• Only business critical systems or processes will warrant consideration for paying a ransom. • Noncritical systems and processes where regulated or sensitive data have not been exposed will warrant no further action. • This will require support from senior management to unilaterally prioritize and identify business-critical systems and processes (and their supporting subsystems) across the entirety of the enterprise; this will reduce the scope of what needs to be protected, allowing the organization to focus resource and financial investments for the purposes of risk optimization. • Although investments will still need to be made for the common IT-related business programs and infrastructure, the scope can be reduced to focus only on those business-critical systems and processes, allowing the organization to make an informed decision.	• The enterprise will get caught off guard; react, not respond; and lose productivity, valuable time, stakeholder confidence and public trust. • The enterprise incident-response costs will increase. • Enterprise employees will experience burnout. • The enterprise insurance carrier will most likely delay, deny and defer the claim because the enterprise was not adequately prepared. • The enterprise has accepted 100 percent of the responsibility and accountability for something that it either did not fully understand or has mistakenly assumed would never happen to it.

Management

Management has the responsibility to set the strategy and dedicate the resources necessary to develop an effective ransomware defense. **Figures 6**–**9** show the multitude of roles, programs, processes and technologies needed to implement and maintain the strategy.

FIGURE 6: Enterprise Roles Required to Support Operations and Strategy

People		
Application Architect	Enterprise Architect	Ransomware Negotiator
Application Dev Team	Forensic Analysts	Reverse Engineer
Chief Financial Officer	Human Resources	Risk Analyst
Chief Information Officer	Insurer	Security Architect
Chief Information Security Officer	Internal Audit	SOC Team
Chief Operating Officer	IT Architect	Systems Administrator
Chief Privacy Officer	Legal Counsel	Threat Intelligence Analyst
Chief Technology Officer	Line of Business	
Data Privacy Officer	Network Engineer	

FIGURE 7: Programs Required to Support Operations and Strategy

Management Programs		
Asset Management	Human Resources Security	Risk Management
Business Continuity & Disaster Recovery Management	Identification & Authentication Management	Secure Engineering & Architecture
Capacity & Performance Planning	Incident Management	Security & Privacy Governance
Change Management	Information Assurance	Security & Privacy Management
Cloud Security Management	Information/Cybersecurity Standards	Security Awareness & Training Management
Compliance Management	Maintenance	Security Operations
Configuration Management	Mobile Device Management	Staff Skills Management
Continuous Monitoring	Network Security Management	Technology Development & Acquisition
Cryptography Management	Patch Management	Third-Party Management
Data Classification & Handling Management	Physical & Environmental Security Management	Threat Management
Embedded/Smart/IoT Technology Management	Privacy Engineering & Architecture	Vulnerability Management
Endpoint Security Management	Project & Resource Management	Web Security

FIGURE 8: Processes Required to Support Operations and Strategy

Processes		
Access Control	Electronic/Cryptographic Key	Risk Assessment (Ransomware specific)
Asset Inventory (inclusive of): • Accounts (Human & Nonhuman) • Applications • Cloud • Data, Information & Knowledge • Hardware • Supply Chain/Third-party	Enterprise Architecture	Risk Management
Application Access Control	Identity and Access Review	Secure Software Development Life Cycle
Application Engineering	Incident Management	Security Awareness & Training Management
Asset Management	Incident Response	Security Engineering
Business Impact Analysis	Information Cybersecurity Policy Development	Security Strategy Development & Alignment
Business Process Engineering	Information/Cybesecurity Procedures	System Access Control
Centralized Logging	Information/Cybersecurity Process Management	Threat Intelligence Management
Change Management	Information/Cybersecurity Standards	Threat Modeling
Configuration Management	Patch Management	User Access Review
Continuous Monitoring	Privacy Impact Assessment	Vulnerability Management
Crisis Communication	Privileged Account Review	
Data Backup & Recovery Testing	Ransomware Negotiations	
Data Classification, Handling & Inventory	Ransomware Playbooks	

FIGURE 9: Technology Required to Support Operations and Strategy

Technology		
Access Controls	End-Point Detection & Response	Network Discovery Scanner
Antivirus/Antimalware	End-User Controls	Network Forensic Tools
Asset Inventory System	File Integrity Management	Network Monitoring System
Baseline (User & Network) System	Full Packet Capture	Network Segmentation
Centralized Logging	Honey Pots/Tokens	Password Manager
Configuration Management	Host Forensic Tools	Patch Management
Data Analytics, Mining & Visualization	Information Sharing Platform	Sandbox
Data Encryption	Intrusion Detection/Prevention System	Security Incident & Event Management System
Data Loss Prevention	Memory Forensic Tools	System Hardening
Detection & Response	Middleware Management	Threat Intelligence Platform
Directory Services	Multi-Factor Authentication	Vulnerability Scanner
Encryption At Rest	NetFlow Capture	Web Application Firewall
Encryption In Transit	Network Access Controls	Web Proxies

Key Roles

Preceding a successful ransomware attack, it is important to identify key roles in the enterprise business, processes and technologies (**figures 6**–**9**) that may typically be involved. These roles need to be clearly documented, understood and communicated, and staff adequately trained to ensure an effective and efficient response. The following are typical key roles:

- **Incident-Response Team**—The team is tasked with investigating the incident, determining the extent of the compromise, collecting evidence, and leading containment and eradication efforts. This team may include the internal or external staff responsible for incident response and digital forensics. It is highly advisable that all work is performed in consultation with legal counsel to attach attorney-client privilege to potentially sensitive communications.
- **Legal Counsel**—Internal and external counsel have the key role of coordinating with all teams in order to understand the details of the incident and provide legal advice on all aspects of resolution.
- **Crisis Communication**—Well-versed in handling crisis events, this individual or team works with counsel to develop and then communicate authorized information regarding the incident to internal and external stakeholders, as appropriate.
- **Ransom Negotiator**—Aligned to the official enterprise ransomware policy, this individual is the primary point of contact in communicating and negotiating the ransom. This individual can be internal to the enterprise or a retained negotiator.
- **Insurance Provider**—Upon notice, an insurance carrier will request information and assess the details of the incident in order to determine applicability of the policy.

Processes and Objectives

The ability of an enterprise to successfully navigate and manage a ransomware attack relies on its ability to quickly identify and respond. The faster it can identify an attack, the faster it can respond, reducing both long-term impacts to business operations and dwell time of the adversary. Well-defined processes and procedures help an enterprise to contain and remove threats sooner.

While the processes and objectives of recovery from a ransomware attack are generally similar to those in incident-management programs, specific attention must be given to the unique details of a ransomware

attack. The key phases of ransomware management are as follows:

- Planning and Preparation
- Detection/Identification
- Containment
- Eradication
- Recovery
- Postmortem/Assessment

Each phase should be defined and tailored to the organization, taking the following considerations into account:

- **Visibility**—The ability to detect indicators that could lead to ransomware incidents, visibility refers to the instrumentation, defined processes, documented procedures, and appropriately skilled and competent staff necessary to recognize the indicators of ransomware attacks and to identify whether the attack is a variant strain of known commodity ransomware or from a big game hunter moving within the environment.

  The type of attack determines what indicators may be present, and whether they are hashes associated with first-stage file droppers and scants/probes of Internet-facing, business-critical systems, phishing attempts against privileged personnel or illicit activity against internal business-critical systems.

The type of attack determines what indicators may be present.

  Visibility allows companies to quickly respond rather than react to a threat, and therefore typically requires an intimate understanding of both the business and technical aspects of an organization. Having established baselines to determine good from bad is essential and requires that organizations have identified and are actively monitoring their environments.

- **Initial Investigation and Analysis**—The objective of initial investigation and analysis processes is two-fold: early detection and faster response to active and present threats to the organization, and preemptive defensive measures to reduce and manage the overall attack surface of the enterprise.
- **Preventing Lateral Movement**—This supports the containment phase activities and the ability to reduce and limit access of the threat actor within the environment by isolating infected devices and reducing the threat actor ability to laterally move within the network. Network segmentation and zero-trust adoption can reduce the attack surface, but enterprises should be aware that, in the most enterprise ransomware incidents, trusted relationships between users, devices and networks are leveraged by the ransomware operators, and in many cases internal domains controllers, DNS servers, or DHCP servers were used to deploy ransomware, bypassing most network segmentation measures.
- **Impact Analysis**—In the situation when detection and response measures failed to detect a ransomware deployment, assessing the impact on data and systems is an activity that needs to be balanced with the impulse to restore data and systems from backups (if backups were not destroyed in the attack). Enterprises should prioritize recovery and investigation activities based on their resilience plans and regulatory requirements. Organizations should be aware that restoring systems and data before collecting forensic artifacts for analysis will lead to the destruction of valuable evidence for the incident investigation and reduce the ability of the forensic investigators to understand how the attack unfolded. Organizations operating in regulated sectors should consider any reporting requirements (e.g., disclosure of data breaches that impact personal information, etc.) and determine how to balance the recovery and response/investigation activities.
- **Determining What Data Were Accessed**—Knowledge of the systems that process, store, transmit or have access to sensitive and regulated data is critical. This requires having current data flow diagrams, accurate asset inventory and a network architecture that demonstrates how data flows within the organization and knowing data owners and business process owners who are affected.

Determining what data were accessed requires having current data flow diagrams, accurate asset inventory and a network architecture that demonstrates how data flows within the organization and knowing data owners and business process owners who are affected.

  Controls and instrumentation, such as data loss prevention, data discovery systems, identity and access management systems, centralized logging and network and user behavior analytics are often leveraged to determine what data may have been accessed or exposed, and what accounts were used to determine the breadth and depth of the adversary's time in network.

  Capabilities employed include incident response and digital forensic efforts; these need to be tailored to the environment and integrated with business operations. Defined processes, procedures and training of associated staff should be documented. Additionally,

senior management (e.g., COO, CIO, CISO, CRO, CFO) should be included to make key decisions, remove roadblocks, and prioritize response efforts for the incident response and forensic team requests (CIO and CISO), assess potential business impact (CRO) and approve financial disbursements (CFO).

Staff involved should include the appropriate senior management members, legal counsel, incident response and forensic team members, and the affected data owners and business process owners; additional staff may be included on an as-needed basis.

- **Were Data Exfiltrated?**—Being able to know if data were exfiltrated from the environment often means the difference between declaring a data breach and mandatory notification, and not having to report. This determination is an important distinction because unauthorized access alone (system or data, interactive or programmatic) does not imply data were exfiltrated. To determine whether exfiltration occurred requires being able to recreate the steps a threat actor took while they were within the enterprise network, which requires sufficiently detailed and properly architected logging solutions to be in place. Additionally, common trace artifacts can exist on system and within the network that indicate data exfiltration (e.g., recently created and then deleted compressed files, file transfers to unknown destinations, and memory-resident applications). Ensuring that incident response and digital forensic processes and procedures, and the team's capabilities, meet organizational requirements is essential. They need to be able to demonstrate that information is being provided and conveyed to key decision makers.

Being able to know if data were exfiltrated from the environment often means the difference between declaring a data breach and mandatory notification, and not having to report.

Controls and instrumentation, such as NetFlow, directory services, IAM systems, full packet capture platforms, SIEMs and properly configured log settings, are often used to recreate the activities of an adversary on the network. System forensic tools can be used to identify the creation and deletion of files that were staged for exfiltration.

Capabilities employed include incident response and digital forensic efforts that are built on defined processes, procedures and training of associated staff.

Staff involved should include the appropriate senior management members, incident response and forensic team members, network architects and engineers, system maintainers, and the affected data owners and business-process owners. Additional staff may be included on an as-needed basis.

- **Business Resumption**—Business recovery efforts should begin after containing the ransomware. This process is unique to each attack and the enterprise official policy on ransomware.
- **Data Recovery**—If the enterprise official policy on ransomware is to pay no ransom, after the threat actor is contained AND eradicated from the environment (and all access methods closed off to the attacker), the business can confidently recover data from immutable backups and resume operations.
- **Negotiated Recovery**—Enterprises need to ensure that they are ready to negotiate the potential recovery of their data (if their official ransomware policy is to pay). Be mindful that payment is no guarantee that any data will be recovered.
- **Negotiations**—Based on a threat actor's skill, resources and level of sophistication, the enterprise may be able to negotiate a lower amount than what is being asked. An identified, trained and skilled negotiator can mean the difference between data loss and recovery. Some basic considerations prior to attempting negotiations include:
  - Do not open the ransomware email or click links; normally, the clock may only start after the first exchange occurs between the enterprise and threat actor.
  - Contemplate possible outcomes; determine the best-case and worst-case results. Then plan how the enterprise would respond to each outcome.
  - Establish an open communications channel (preferably outside of the primary channel because the enterprise network is now compromised). This communication team should include senior management and legal counsel.
  - Verify if the threat actor is listed on the sanctions list maintained by the Office of Foreign Asset Control[6] to prevent introducing additional risk to the enterprise. This should be done by legal counsel.
  - Leverage the enterprise threat intelligence program, including threat intelligence data from established communication

6 U.S. Department of the Treasury, "Office of Foreign Assets Control—Sanctions Programs and Information," https://ofac.treasury.gov/

channels with law enforcement. For example, to understand the threat actor, get answers to the following questions:

- How have they handled ransoms in the past?
- Are they reliable in delivering decryption keys that will recover the data or are they more akin to smash-and-grab criminals?

- **Threat Actor Communications**—Big game hunters tend to be financially motivated. They often make significant investments to gain access and spend weeks understanding an enterprise's networks and business operations before launching an attack. They invest in supporting infrastructure (i.e., call centers) to walk an enterprise through the process of setting up crypto accounts to make payment. Negotiations may be quickly resolved. They may also be protracted, taking time for offers and counter offers to be made before coming to an agreement. It is strongly advised that enterprises do not underestimate a threat actor who is holding their data for ransom, and do not attempt to intimidate or threaten them. Remember, every hour the enterprise is without its data is an hour of business interruption.
- **Crypto Payment Transfer Obfuscation**—Enterprises should not make ransom payments directly from their corporate account(s). There is the chance that the threat actor may not recognize the enterprise during the transaction (even though they have spent time in your environment). This may work in your favor, because they may not correlate that the enterprise is willing to pay and may not attempt to return in the future. A recent study[7] reports that 80 percent of enterprises that paid a ransom were attacked with ransomware a second time, with 40 percent paying again. Seventy percent of these paid a higher amount for the second incident.

Public Communication and Disclosure

Critical to successfully navigating through the incident-response process in the wake of a ransomware attack is asking whether and how to communicate with internal and external stakeholders. This requires clear, intentional messaging tailored to the different audiences. This should be done by individuals (carefully selected and trained prior to the event) working in consultation with legal counsel to help ensure that messaging is delivered in a timely, context-appropriate manner that does not obfuscate, misrepresent or mislead.

Law Enforcement—Work with legal counsel to establish these relationships in advance of an incident. Get to know who will be working with the enterprise, when the enterprise is authorized to contact them, what their capabilities are to support the enterprise, and what level of detail the enterprise is permitted to share. This should be documented and kept current.

Regulatory Bodies—Work with legal counsel to identify any disclosure requirements under applicable law, including the timing, substance, and recipients of any disclosures. While notification is dependent upon the application of laws to the facts, this notification chart should be documented and maintained to align with evolving legal and regulatory developments.

Insurance Provider—Work with legal counsel to identify the enterprise's points of contacts, including what information must be disclosed under the policy (and when).

Public Inquiries and Public Media—Work with legal counsel, crisis management, corporate communications, the public relations firm, customer support services and the social media department to ensure that only approved messaging that accurately reflects the incident is shared. Legal counsel should review the message to

7 ContinuityCentral.com; "80 percent of organizations that paid a ransom demand were hit again," 9 June 2022, http://www.continuitycentral.com/index.php/news/technology/7383-80-percent-of-organizations-that-paid-a-ransom-demand-were-hit-again

Case Study: Colonial Pipeline Ransomware Attack

In May 2021, Colonial Pipeline experienced a ransomware attack. Initial access was gained to the Colonial Pipeline network when criminals exploited a legacy virtual private network (VPN) that should not have been in use.

In addition to impacting internal business operations, this incident had a far greater reach, impacting other industries (i.e., commercial air travel) and initiating panic buying with at least 17 states over a four-day period.

Although there are questions about how a legacy VPN system without multifactor authentication (MFA) was still in use, Colonial Pipeline leadership did not attempt to dodge responsibility or deflect blame for the resulting incident. They identified the cause and worked to address the matter in a manner that they felt at the time was in the best interest of their stakeholders.[8]

Case Study: The Guardian Ransomware Attack

On 20 December 2022, *The Guardian* was hit by a cyberattack incident believed to be a ransomware attack. In January 2023, The Guardian confirmed that the attack was ransomware, and that UK staff-member personal data were accessed. News staff were able to continue producing a daily newspaper while working from home until the IT staff completed system restoration. *The Guardian* hired "external experts to gauge the extent of the attack and to recover its systems."[9] Management informed the public and staff of the disruption associated with the operations.[10]

Case Study: Rackspace Attack

On 2 December 2022, customers of the cloud computing giant Rackspace began experiencing outages relating to their Hosted Exchange Server. Very little information was shared regarding the outage impacting several thousand customers beyond stating it was "a security incident" after deciding to "power down and disconnect" the service.[11]

In its regulatory filing, Rackspace states, "The Hosted Exchange Email business represents approximately 1% of Rackspace's total annual revenue and is comprised of primarily small and medium businesses who solely use this product. No other Rackspace products, platforms, solutions, or businesses were affected or are experiencing downtime due to this incident."[12] While this can be viewed as good news for Rackspace and perhaps its larger clientele, it does little for smaller enterprises reliant upon solution providers in the first place. Rackspace public statements regarding corporate preparedness conflict with what reportedly enabled the attack to occur – failure to patch for CVE-2022-41080 and CVE-2022-41082.[13, 14, 15] Worse, Rackspace has seemingly blamed its decision not to patch based on characterization by Microsoft.[16, 17] Regardless of reason, customers were unhappy resulting in at least two lawsuits.[18]

The Rackspace ransomware incident illustrates how the mishandling of an incident can influence public sentiment. Additionally, it highlights the importance of good crisis communications and empathy.

8 David Sanger; Krauss, Clifford; Perlroth, Nicole; "Cyberattack Forces Shutdown of a Top U.S. Pipeline," *New York Times*, 8 May 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

9 Milmo, Dan; "Guardian Confirms it Was Hit by Ransomware Attack," *The Guardian*, 11 January 2023, http://www.theguardian.com/media/2023/jan/11/guardian-confirms-it-was-hit-by-ransomware-attack

10 Waterson, Jim; "Guardian Hit by Serious IT Incident Believed to be Ransomware Attack," *The Guardian*, 21 December 2022, http://www.theguardian.com/media/2022/dec/21/guardian-hit-by-serious-it-incident-believed-to-be-ransomware-attack

11 Beaumont, Kevin; "Rackspace Cloud Office suffers destructive security breach," DoublePulsar, 2 December 2022, https://doublepulsar.com/rackspace-cloud-office-suffers-security-breach-958e6c755d7f

12 MarketScreener, US Securities and Exchange Commission, "Rackspace Technology: Regulation FD Disclosure – Form 8-K," 9 December 2022, http://www.marketscreener.com/quote/stock/RACKSPACE-TECHNOLOGY-INC-110370321/news/Rackspace-Technology-Regulation-FD-Disclosure-Form-8-K-42514786/

13 Kovacs, Eduard; "Rackspace Completes Investigation Into Ransomware Attack," Security Week, 6 January 2023, http://www.securityweek.com/rackspace-completes-investigation-ransomware-attack/

14 Culafi, Alexander; "Rackspace: Ransomware attack caused by zero-day exploit," TechTarget, 4 January 2023, http://www.techtarget.com/searchsecurity/news/252528884/Rackspace-Ransomware-attack-caused-by-zero-day-exploit

15 Robichaux, Paul; "What We Can Learn from the Rackspace Breach," Practical 365, 19 January 2023, https://practical365.com/what-we-can-learn-from-the-rackspace-breach/#:~:text=Rackspace%20didn't%20install%20the,2022%2D41082%20was%20remotely%20exploitable

16 *Op cit* Kovacs

17 "Rackspace blames Microsoft over ransomware attack," The Stack, 6 January 2023, https://thestack.technology/rackspace-blames-microsoft-exchange-zero-day/

18 Kovacs, Eduard; "Rackspace Hit With Lawsuits Over Ransomware Attack," Security Week, 12 December 2022, http://www.securityweek.com/rackspace-hit-lawsuits-over-ransomware-attack/

prevent providing too much information and to ensure that information that needs to be safeguarded is not disclosed.

Media relations should always be handled delicately. Never assume that information disclosed is off the record. Ensure that only those individuals who have been trained and are authorized to speak with the public are sharing the messaging. This safeguard reduces the chance of accidentally revealing too much information, especially if the investigation involves law enforcement and is ongoing. Ensure that your social media department and customer support services are prepared and trained on how to respond and handle public inquiries or statements being made on social media platforms. Playbooks, processes and procedures must be documented and maintained. Training needs to be conducted periodically to refresh knowledge and responses tested to ensure that they are properly aligned.

A communication/disclosure strategy is important for both short-term and long-term impact, and leadership must:

- Demonstrate their resolve and commitment to corrective actions.
- Announce the incident.
- Be honest and act with accountability.

Assurance

Ransomware Readiness Assessment

This section aims to help organizations ensure adequate preparedness for a ransomware attack. The following guidance and steps can help organizations enhance their readiness and response capabilities.

1. **Governance**—To prepare for a ransomware attack, the organization governing body (e.g., board of directors or board of regents) needs to ensure that proactive steps are in place to determine not only the enterprise's ability to respond to the incident, but also its level of readiness.

   Historically, this has meant increasing cyberinsurance. However, more insurance providers are pulling coverage from ransomware incidents[19] or instituting much stricter underwriting requirements[20] (i.e., objectively demonstrable proof of sufficient, not merely adequate, programmatic management of information security and privacy efforts within the organization). Response readiness requires the enterprise to prioritize and potentially overhaul the management of staff, processes and technologies used to defend it.

   To gain the desired level of assurance, enterprises can consider leveraging the *Ransomware Readiness Audit Program*,[21] a vendor-agnostic approach to determining the overall readiness of an enterprise to address ransomware attacks. This program helps senior management and management teams increase their operational efficiencies and reduces the chance of insurance claims being denied because they know where the enterprise should focus its ransomware protection resources.

2. **Management**—Management must understand which data assets the enterprise most needs and values (both on-premises and with third-party providers) and clearly account for risk ransomware poses to those data. Managing an organization's ability to effectively and efficiently respond to a ransomware attack requires viewing the risk across the spectrum of attack categories, re-evaluating its operational posture, and ensuring systems and network hygiene.

19 Cohn, Carolyn; "Insurers Run From Ransomware Cover as Losses Mount," Reuters, 19 November 2021, http://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/

20 Violino, Bob; "Rising Premiums, More Restricted Cyber Insurance Coverage Poses big Risk for Companies," CNBC, Technology Executive Council, October 2022, http://www.cnbc.com/2022/10/11/companies-are-finding-it-harder-to-get-cyber-insurance-.html

21 ISACA, Ransomware Readiness Audit Program, 2022, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000005uz6vEAA

3. **Information Protection Processes and Procedures**—Organizations that prioritize and plan for a ransomware attack need to ensure that they have the appropriate processes and procedures in place.

   Operationally, enterprises have relied heavily on undocumented knowledge to sustain business. Processes and procedures need to be written down and those records kept current to ensure that, in the event of an incident, responding and recovery are done in the most effective and efficient manner feasible.

   Enterprises must look objectively at their IT and security architectures and identify gaps to ensure that business continuity and disaster-recovery efforts consider and account for ransomware attacks.

4. **Technology Controls**—The problem with the acquisition and implementation of technology controls stems from the lack of full integration of those controls within enterprise business operations.

   Although some technology controls may be easy to acquire, such as a new endpoint detection and response (EDR) or data loss prevention (DLP) solution, other technology controls require significant thought, consideration of execution and re-engineering of technology and business workflows (e.g., introducing segmentation of an existing network environment).

   Ransomware attacks leverage an enterprise's controls and control gaps against it. Attackers are successful because a gap exists. Not only must tools be properly attuned to the environment, but staff must be properly trained on tool capabilities and how to operate them.

5. **Human Controls**—The most difficult aspect of ransomware readiness is likely to be the human element because organizational culture drives the success or failure of ransomware readiness plans and efforts.

   In order for human controls to succeed, an enterprise must ensure that staff are aware of the various tactics, techniques and procedures (TTPs) of attackers, the potential impact of an attack and who to contact. Enterprises must also ensure that all contacts are aware of the approved actions and steps to be taken and how to escalate such incidents.

   Senior management needs to make human controls a priority and remind and train everyone on the parts they play in protecting the organization.

Ransomware Readiness Testing

1. **Tabletop Exercises**—Tabletop exercises are an essential part of an organization's cybersecurity preparedness program, particularly given the rapidly changing capabilities of attackers. These exercises simulate real-world cybersecurity incidents and allow different parts of the business to test their response capabilities and refine their incident-response procedures. Key to a successful tabletop engagement is involving the right stakeholders. It is important to ensure the gaps are identified and addressed based on an internal risk-impact prioritization scale. It is recommended that these testing methods be performed periodically throughout the year. These exercises can help organizations understand the evolving threat landscape, practice incident-response procedures, foster a culture of cybersecurity awareness and demonstrate their preparedness to stakeholders.

2. **Simulation**—These testing methods are a bit more invasive in nature and are meant to test control efficacy and aid in identifying overall readiness strengths and potential gaps that may exist within the environment.

   Simulations should be leveraged to verify and validate management assertions of business resiliency, continuity, incident-response and disaster-recovery capabilities. To provide the level of assurance required by the governing body and senior management, simulations must be conducted in context of technical operations. It is recommended that simulations be conducted in context of technical business operations and business impact analysis, identifying impacted systems involved with the simulation. During the simulation, staff from business and IT should be able to quickly identify impacts.

   Simulations could be planned or covert. Planned simulations should be well coordinated to minimize the impact to the business while meeting the goal to identify, document and assess in a controlled manner. Done properly, simulations will allow enterprises to develop appropriate corrective actions and mitigation steps not previously known or identified. The purpose of covert simulation is to test the organization response to real attacks.

Ransomware Readiness Training

1. **End Users**—It is important to ensure that everyone on staff knows what their responsibilities are, and when and how to perform them. Ransomware attacks may go unreported simply because the end user does not know who to contact, thinks that IT is taking care of the issue or does not trust that the Help Desk staff will help them.

   Ransomware attacks often begin by targeting end users. Attackers know that end users are the last line of defense. Senior management needs to ensure that end users are aware of threats, know the steps to take if they suspect illicit activity, and report it in a timely manner to reduce the impact and effects of a ransomware attack. End-user education and awareness must be of sufficient frequency to address organizational needs.

2. **Information Technology**—Given their increased privileges, access and reach within the environment, IT staff must be made aware and reminded that they are frequent targets of attackers. They need to be trained on how to engage with the respective incident response and cyber and information security teams if there is a suspected ransomware event.

   IT staff fill multiple roles when addressing the threat of ransomware. They should have a solid understanding of supporting playbooks/standard operating procedures that define the activities and steps that management has already deemed permissible, the actions that require management approval, and escalation paths and associated timelines to reduce adversary dwell time on a system or within the network and diminish the spread and impact of an attack. They need to be intimately familiar with the operating environment to better support incident-response capabilities, specifically those relating to containment, eradication and recovery efforts.

3. **Ransomware Incident Responders**—Effective and efficient responses to ransomware require specific training, skills and competencies. It also requires sufficient planning and preparation, based on the enterprise ransomware policy (i.e., the official stance on paying ransom).

   Numerous attackers and a wide range of ransomware strains exist, and responders may not know what they are facing until they are actively engaged. Responders need to keep their skills and competencies relevant to current ransomware.

   Figure 10 shows common skills and competencies associated with ransomware incident-response efforts.

FIGURE 10: Common Ransomware Incident-response Skills

Personal Skills	Technical Skills
Ability to follow directions, policies and procedures	Adversary tactics
Collaboration	Identifying forensic artifacts
Communication (written and oral)	Incident analysis
Diplomacy	Incident handling skills
Documentation	IT and security architecture
Integrity	IT and security engineering
Investigative	Malicious software
IR life cycle	Monitoring
Knowing one's limits	Network applications and services
Leadership	Network operating systems
Maintenance of incident records	Network protocols
Presentation	Operating systems
Problem solving and persistence	Programming
Self-awareness	Security issues (network and host)
Stress management	Security principles
Time management	Security vulnerabilities/weaknesses

Conclusion

Having a defined strategy and roadmap to reduce the likelihood of a large-scale attack is the first step in exposing a ransomware attack for what it truly is—an avoidable disaster. This requires preparation. When enterprises have established a defined strategy for ransomware that is managed within the level of risk they are prepared to accept, well-informed decisions can be made. If a ransomware incident occurs, it will be managed within the risk appetite of the business and well-informed decisions will be made.

In the past, enterprises attempted to transfer ransomware risk to insurance carriers, but today providers are instituting much stricter underwriting requirements or pulling coverage altogether. A ransomware attack is just another risk an enterprise needs to consider and address.

A ransomware strategy ensures that the enterprise is ready for a ransomware attack and defines desired goals and objectives in the context of a potential attack. If one objective is to ensure quick recovery, it needs to invest in and validate (i.e., test, test, test) the ability to recover business-critical assets. If an enterprise is open to negotiating with an extortionist to get back its data, then it needs to have cryptocurrency ready so it does not lose precious time.

Knowledge Check: CPE Quiz

Test your knowledge on ransomware defense by taking this quiz: https://www.isaca.org/resources/white-papers/blueprint-for-ransomware-defense-cpe-quiz. ISACA members earn 1 CPE credit by passing with a score of 75%.

ISACA values your input: https://www.research.net/r/VPKKJN3.

Acknowledgments

ISACA would like to recognize:

Lead Developer

Edward McCabe
CISM, CGEIT, CRISC, CDPSE, COBIT, ISO/IEC 27K1 ISMS LI, SABSA
Founder/Principal, The Rubicon Advisory Group
USA

Expert Reviewers

Joyce Chua
CISA, CISM, CDPSE, CIMP, CAEG (Professional), FIP, CIPP(E), (C)CISO, CIPM, CIPP(A), CFE, CIA, PMP, ITIL, MCP, IRCA ISMS Associate Auditor
First Vice President, UOB
Singapore

Sergiu Sechel, Ph.D.
CISA, CISM, CRISC, CFE, CEH, CBP, CSSLP, CDPSE, GICSP, GPEN, GWAPT, GCFA, GNFA, GASF, GCTI, GREM, PMP
Boston Consulting Group
UK

Ramona Ratiu
CISA, CISM, GSTRT, MS
Cyber Security Manager–Zurich Insurance
Adjunct Professor– DePaul University
USA

Manjunath A.T
CISA, CSA, CCSK
IT Compliance Auditor, Applied Materials
India

Julia Hermann
CISM, CDPSE, CISSP, CCSP
Head of Security Architecture and Cyber Defense,
Giesecke+Devrient GmbH
Germany

Kevin Fumai
CDPSE, CIPP/US/E, CIPM, CIPT, FIP, PLS, CCSK, CEET
Assistant General Counsel,
Oracle America, Inc.
USA

Board of Directors

Pamela Nigro, Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

John De Santis, Vice-Chair
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP
Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, Germany

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Maureen O'Connell
NACD-DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Veronica Rose
CISA, CDPSE
Senior Information Systems Auditor–Advisory Consulting, KPMG Uganda, Founder, Encrypt Africa, Kenya

Gerrard Schmid
Former President and Chief Executive Officer, Diebold Nixdorf, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd., Israel

Gregory Touhill
CISM, CISSP
ISACA Board Chair, 2021-2022
Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick
ISACA Board Chair, 2020-2021 and Interim Chief Executive Officer

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM, NACD-DC
ISACA Board Chair, 2018-2019
Independent Director, Titus, Executive Chair, White Cloud Security, Managing Director, Clyde Consulting LLC, USA

About ISACA

ISACA® (https://www.isaca.org/) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 170,000 members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *Blueprint for Ransomware Defense* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:
https://www.research.net/r/VPKKJN3

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/