Ransomware Incident Response: Managing in Minutes
An Introduction to the SANS Institute’s PICERL Approach

Abstract

With cybersecurity threats on the rise, organizations must be ready to address a new set of security challenges and considerations, including increasingly serious threat actors, a larger attack surface from the exponential growth in connected devices, and a proliferation of malware variants. Gone are the days when a lost laptop was the biggest security concern. Health care organizations (HCOs) are attractive, lucrative targets for cyber attackers for several reasons: we have complex IT systems with highly marketable data; we often lack strong and consistent security controls; and the culture of openness and helpfulness in health care can make us unwitting targets.

Ransomware has seen a significant uptick in attacks in 2016 and can inflict severe financial, operational, and reputational damage upon its victims. A recent HIMSS Analytics survey found that about 50% of hospitals have been targeted by ransomware in the past year. Now, more than ever, it is critical to ensure your organization has a proper response plan in place for cybersecurity incidents. The SANS Institute, a renowned security research and training organization, introduced PICERL as an incident response methodology. It has been praised as a go-to response approach for organizations because of its applicability and versatility across industries, organization size, and type of security incident.

This note will introduce and broadly define the six phases of SANS Institute’s PICERL methodology: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. While this approach can be applied for any cyber incident, we will use ransomware as an example throughout.

SANS Institute’s Six-Step PICERL Approach

Execute in minutes

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned

Monitor Systems

Continuing Improvements
- Educate, train, and test users
- Tweak existing tools
- Integrate new indicators
- Acquire new technology

Sources: SANS Institute, SANS.org; Health Care IT Advisor research and analysis.
Authors: Allyson Vicars, Ernie Hood
Published: November 2016
Ransomware Incident Response: Managing in Minutes

Six-Step PICERL Approach

Preparation

The Preparation phase sets the foundation for how the organization will manage cybersecurity threats. In this phase, organizations can take several steps to bolster their cyber defenses; a few of them are listed here.

- **Ensure appropriate internal policies and procedures** are in place to address and manage incidents (e.g., who has the authority to communicate with impacted consumers and staff; define the responsibilities to ensure preparedness such as testing response plans regularly or maintaining checklists and templates).
- **Establish a multi-disciplinary incident response team (IRT)** with IT and non-IT stakeholders—including the CISO, CIO, CMO, and CFO—and predefine roles and scope of responsibilities for when incidents do occur. Establish who chairs the team and who are voting members.
- **Conduct risk assessments and audits** to ensure threats can be identified early.
- **Implement and/or strengthen web and email gateways** (sometimes called proxies) for network-connected workstations and devices to limit end-user access to harmful websites and emails. Most incidents of ransomware have occurred as a result of a staff member clicking on a link that activates the malware.
- **Invest in awareness training and testing** (e.g., faux-phishing campaigns). Even organizations with robust cyber defense systems are at risk due to human error or misjudgment.
- **Use non-drive-mounted backups and test them on a regular basis.** They are a critical part of thorough preparation for a cyberattack from a business process perspective.
- **Train and drill users on downtime operating procedures.**

Identification

The Identification phase begins when an HCO discovers a cybersecurity threat on their network or on a user’s computer. HCOs may discover malware attacks and breaches in a variety of ways.

- **Intrusion detection systems (IDS)** can scan computer and network traffic for suspicious activity to help identify threats.
- **Users** may notify IT operations of issues, such as a locked and inaccessible computer after a ransomware incident.
- An IT or security operations audit of security logs may reveal an attack.
- **Audits of workstations and networked systems** can also uncover cybersecurity incidents, but shared workstations pose a particularly high risk and should be monitored frequently.

Note that the Identification phase is a continuous process and HCOs should actively monitor their network for threats. It is critical to ensure your organization has the capacity and resources in place to quickly identify the type of threat involved.

Containment

In the Containment phase, a ransomware incident has been identified, and immediate action must be taken to isolate the infection before it spreads to other machines or completes its malicious activity. By the time IT arrives at the scene, it is too late—users must be trained on actions they should take in the seconds following the realization that there is a problem. HCOs must be ready to manage incidents in mere minutes as many ransomware strains attempt to breach other machines on the network once they are activated. Depending on the magnitude of the event, the IRT may be called upon to manage the situation once the security team has
Six-Step PICERL Approach, continued

contained the infection. IRTs are critical because they enable a coordinated response to important and time-sensitive decisions. Clear lines of decision-making authority and provisions for backup decision makers should be made in advance.

**Eradication**

16% Of IT executives who have never experienced a breach would pay the ransom.

43% Of IT executives who have experienced a breach would pay the ransom.

The **Eradication** phase represents the organization’s cleanup process for an infected device, workstation, or network. The process varies depending on the type of cybersecurity threat and the magnitude of the incident. Many cybersecurity experts recommend that any infected device be taken down to bare metal and completely re-imaged—do not expect an antivirus or spyware removal tool to solve the problem. More complicated cases may require third-party involvement to scan all your systems, including backups, to ensure the malware is completely eliminated.

For ransomware especially, backups are the last line of defense so it is vital that leadership be fully aware of the Recovery Point Objectives and Recovery Time Objectives. A crisis is a bad time to explain to leadership that the last backup is a week old and that it will take seven more days to recover from the backup. Backups should be unmounted and otherwise unalterable as certain ransomware variants are known to target and encrypt backups. Recovery should also be tested on a regular basis. A ransomware infection will require the organization to wipe the infected computer, restore the latest backup, and apply any appropriate patches or security changes before reconnecting the machine to the network.

The decision to pay—or not pay—a ransom should not be made by the CISO or information security team alone and should not be made lightly. Many aspects should be considered and one must weigh the potential of immediate relief with the risk of further attacks and additional demands for payment. As the Radware survey data to the left illustrates, respondents who had been hit with ransomware were much more likely to pay than those who had not yet had to deal with it. The Federal Bureau of Investigation (FBI) discourages paying the ransom demand, not wanting to encourage criminal behavior.

An overwhelming number of **ransomware variants** to deal with, including:

- **Locky** Encrypts important files; user must pay ransom to receive decryption key
- **Dridex** Steals banking information and financial credentials
- **Cerber** Encrypts files without Internet access
- **RAA** Encrypts important files and installs password-stealing programs
- **Cryptxx** Affects all versions of Windows (XP, Vista, 7, 8, and 10); found April 2016
- **TeslaCrypt** Affects Windows documents; free decryption key publically available
- **Ranscam** Implements scare tactics to entice victim to pay ransom but does not actually encrypt files
- **Crysis** Runs every time the user logs in to the system, making it more difficult to remove

Sources: SANS Institute, SANS.org; Health Care IT Advisor research and analysis.

©2016 Advisory Board • All Rights Reserved

Six-Step PICERL Approach, continued

Two Decisions in the Face of Ransomware

<table>
<thead>
<tr>
<th>Is It a Breach?</th>
<th>To Pay or Not to Pay?</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2016: HHS(^1) released guidance on ransomware prevention and recovery</td>
<td>The FBI discourages paying a ransom because:</td>
</tr>
<tr>
<td>The presence of ransomware on a computer system is deemed a security incident under the HIPAA(^2) Security Rule</td>
<td>• It encourages the criminal business model</td>
</tr>
<tr>
<td>Covered entities or business associates must initiate their security incident and response and reporting procedures</td>
<td>• It does not guarantee access to stolen data</td>
</tr>
<tr>
<td></td>
<td>• It does not exempt your organization from a second payment demand</td>
</tr>
<tr>
<td></td>
<td>• It does not prevent additional malware that requires additional payments</td>
</tr>
<tr>
<td></td>
<td>• HCOs may be able to negotiate a lower ransom</td>
</tr>
</tbody>
</table>

Recovery

Once the threat has been eliminated from the infected computer or network, the **Recovery** phase begins. Recovery involves running the previously infected computer through a series of validation tests to ensure the problem no longer persists, that it is safe to resume normal function, and that the computer can reconnect to the network without the possibility of re-infection. Validation tests confirm that no gaps or backdoors have been forgotten. HCOs can monitor log files and accounts, and conduct other checks to ensure the computer continues to run without issues.

Lessons Learned

In the **Lessons Learned** phase, organizations should compile documentation and other pertinent information about the cybersecurity incident. The IRT should review the case and may decide to make recommendations to leadership if there are any potential gaps or security risks identified as a result of the event. These lessons learned should be leveraged in the preparation phase to improve how the organization readies for threats. Documentation of the lessons learned and improvements made is vital to minimize issues with finance auditors and the OCR.\(^3\)

Case information can also be used to provide future user training and to improve incident response. Incidents provide an opportunity to reevaluate existing monitoring and defense capabilities.

Conclusion

By including a preparation and lessons learned phase, PICERL recognizes it is imperative to review and update security policies after each incident to ensure new threats can be managed appropriately. Since many cybersecurity incidents result in data loss or system downtime, as with ransomware, organizations should view cybersecurity as a business operations problem. A May 2016 LogRhythm report identified that companies affected by ransomware lost access to their data for two to five days.\(^4\) For provider organizations, access to medical records and other data is an integral component of everyday operations. Leadership must find ways to reduce downtime and prepare clinicians and other staff to operate as efficiently as possible when systems are down. Recovery from backups can vary depending on the magnitude of the incident and will impose some downtime. One infected computer may take less than an hour to recover, while an EMR database or network share may take days.

---

1) HHS = US Department of Health and Human Services.  
2) HIPAA = Health Insurance Portability and Accountability Act.  
3) OCR = Office of Civil Rights.  
Next Steps

Action Items

IT leaders should consider the following action items to remain vigilant against cybersecurity threats:

- **Implement PICERL as an incident response methodology for cybersecurity.**
  Review the PICERL documentation provided online via the [SANS Institute website](http://www.sans.org). Introduce the method to key stakeholders within your organization. Review your organization’s current policies to see if you already use this methodology.

- **Educate your C-suite and board about cybersecurity risks and mitigation strategies.** Cybersecurity threats impact every department and operation within an organization. Engage your C-suite and board to understand their concerns and discuss how both can support initiatives. When approaching the C-suite or board for decisions, provide options and alternatives with consequences expressed in business and clinical terms. Ensure that leadership is well aware of recovery time objectives (RTOs) and recovery point objectives (RPOs).

- **Conduct risk assessments and internal phishing campaigns.** Conduct risk assessments and penetration tests regularly to identify potential problems before incidents occur. Internal phishing campaigns, which can be organized and managed by third-party vendors, are valuable tools for raising staff awareness and improving the last line of defense: “the human firewall.”

- **Use email and website filters as well as Internet access controls for workstations.** Apply filters to potentially dangerous email and websites. Consider limiting the number of workstations with Internet access or isolating specific computers.

- **Implement network segmentation.** Segment your network to mitigate intrusion, limit further movement across the network, or limit the propagation of a threat. If your organization has already implemented this control, review your current strategy to ensure it addresses the latest cybersecurity threats.

- **Adopt the “Principle of Least Privileges” approach.** Ensure all employees within the organization have appropriate privileges by providing the lowest level of user rights necessary to complete their responsibilities. Restrict administrative access only to individuals who need to have such access. Deploy special protections for privileged accounts such as multi-factor authentication or check-in/out procedures.

**Recommended Resource**

*How to Build A Breach Plan*

The speed and honesty with which an organization responds can have a great impact on limiting the damage. In this presentation, we focus on the most important things to have in place before a breach occurs.