cyber crucible

Managing Ransomware Risk: An Executive's Primer

What is ransomware?

It’s a type of malware that prevents a user or organization from utilizing their electronic devices and data until a fee – anywhere from thousands to millions of dollars – is paid.

Ransomware is usually spread through phishing emails, hacked websites, or infected files. Many attacks originate from the email addresses of trusted contacts and community leaders who were targeted.

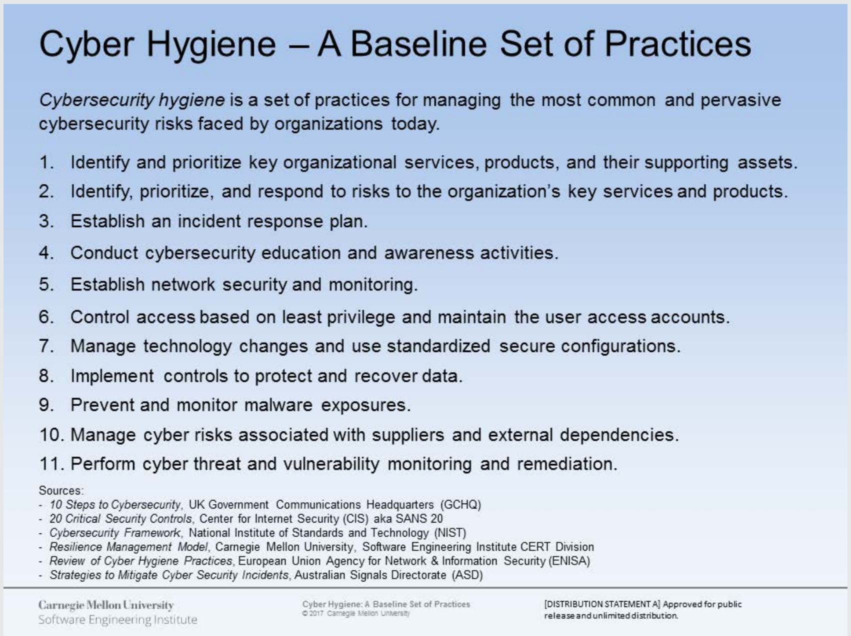
At this point, the criminal begins to crawl through a network looking for valuable data, then encrypting the user or organization’s files, databases, email, and backups – often all at the same time.

It’s not just big businesses that are impacted. The number of successful attacks against non-profits has risen, which means that ransomware is a risk that every executive team needs to address.

The Importance of Prevention

While the prevention of ransomware risk is never foolproof, it is necessary. Think of it this way – you and your team wash their hands to prevent illnesses. In the same way, there are some simple cyber hygiene tasks to limit the chance of ransomware infection.

Matthew Trevors of Carnegie Mellon University's Software Engineering Institute produced some great guidance for cyber hygiene, such as this insightful set of practices.



Cyber Hygiene – A Baseline Set of Practices

Cybersecurity hygiene is a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today.

1. Identify and prioritize key organizational services, products, and their supporting assets.
2. Identify, prioritize, and respond to risks to the organization's key services and products.
3. Establish an incident response plan.
4. Conduct cybersecurity education and awareness activities.
5. Establish network security and monitoring.
6. Control access based on least privilege and maintain the user access accounts.
7. Manage technology changes and use standardized secure configurations.
8. Implement controls to protect and recover data.
9. Prevent and monitor malware exposures.
10. Manage cyber risks associated with suppliers and external dependencies.
11. Perform cyber threat and vulnerability monitoring and remediation.

Sources:
- *10 Steps to Cybersecurity*, UK Government Communications Headquarters (GCHQ)
- *20 Critical Security Controls*, Center for Internet Security (CIS) aka SANS 20
- *Cybersecurity Framework*, National Institute of Standards and Technology (NIST)
- *Resilience Management Model*, Carnegie Mellon University, Software Engineering Institute CERT Division
- *Review of Cyber Hygiene Practices*, European Union Agency for Network & Information Security (ENISA)
- *Strategies to Mitigate Cyber Security Incidents*, Australian Signals Directorate (ASD)

Carnegie Mellon University
Software Engineering Institute

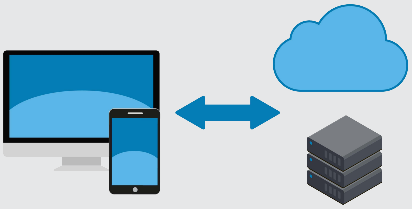
Cyber Hygiene: A Baseline Set of Practices
© 2017 Carnegie Mellon University

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Try these four simple tips to get started:

1. Install some type of antivirus.
2. Enable 2-factor – otherwise known as multi-factor – authentication on all accounts. This means that you must enter a code into your phone in addition to a password on websites.
3. Think before you click on a document or website that looks abnormal. If a message looks odd, call the author before taking action.
4. Always back up your data.

When Prevention Doesn't Work - Restoring From Backups



For many organizations, it's highly likely that some encrypted data has not been backed up. If this fits you – you're not alone. After all, the cost of backing up all of your data can be significant.

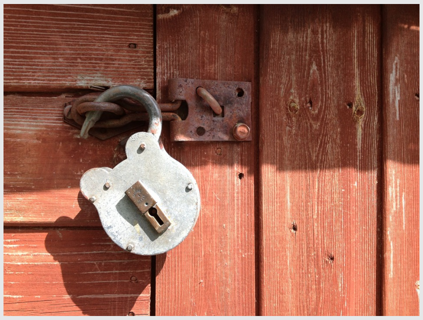
Any risk mitigation strategy should work to prioritize backing up essential data that's essential. That way, you can continue servicing your customers and communities. Former medical practitioners may find this process similar to creating rules for which patient(s) should be the highest priority in an Emergency Room.

Backups – even incomplete or imperfect ones – are a way to avoid paying ransoms. Criminals have adapted and begun encrypting or deleting backups by creating automated attack capabilities in their ransomware tools, as well as manually searching for backups.

Up to 77% of backups fail. That does NOT include ranswomare attacks on backups

"Offline" backups are any form of backup not connected to your network. A good rule of thumb: Any data stored offline can't be easily encrypted. It may contain ransomware, though!

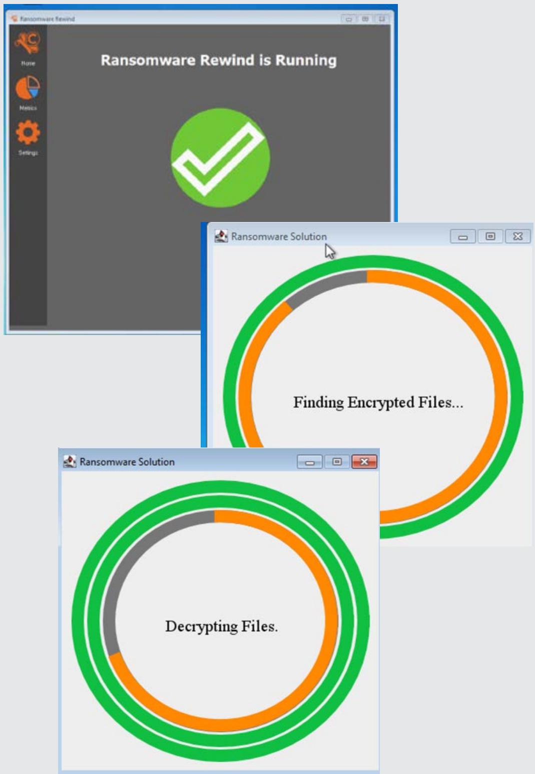
When Prevention Doesn't Work- Decrypting without Paying The Ransom



Decryption is one of the most attractive solutions available after a ransomware attack, but it does mean that prevention methods have failed.

As decryption methods were discovered and made available by security researchers, sometimes with law enforcement assistance, victims of ransomware attack had the option to simply decrypt after an attack. No need to dive into backups, and certainly no need to pay any ransoms.

While all products advertising the ability to rewind ransomware have strengths and weaknesses, we developed Cyber Crucible's own Ransomware Rewind to be an inexpensive and easy-to-use solution. That makes it perfect for smaller companies, non-profits, and large organizations alike.



Ransomware Rewind is Running

Finding Encrypted Files...

Decrypting Files.

cyber crucible

Severna Park, MD 21146
Oakmont, PA 15139
(410) 216-0369

info@cybercrucible.com
CYBERCRUCIBLE.COM
RANSOMWAREREWIND.COM

When Prevention Doesn't Work- Thinking of Paying the Ransom

Nobody likes to negotiate with criminals. This is a very emotional time, yet you have to approach things rationally. This may be an unavoidable solution, if you are out of options, but wish to keep serving your customers.

If you feel forced into this solution, please consider the following:

1. The odds of the criminal not giving you your decryption keys are very low.

2. You may hit some bugs, but the decryptors normally work.

3. Just like any other fraud, you may be opening yourself up to additional attacks from these or other criminals (word gets out).

4. You are at high risk of re-infecting yourself, possibly soon after you spend the time and money recovering.

5. Plan for significant downtime while decrypting files, weeks or months after paying the ransom. Hacker tools aren't necessarily automated.

CryptoLocker

Your important files encryption produced on this com
documents, etc.

If you see this text, but do not see the "CryptoLocker" win
deleted "CryptoLocker" from compute
files, you have to recover "CryptoLocker"
y of "CryptoLocker" in the Interne
ker" from the link give
1002.exe

cyber crucible

Severna Park, MD 21146
Oakmont, PA 15139
(410) 216-0369

info@cybercrucible.com
CYBERCRUCIBLE.COM
RANSOMWAREREWIND.COM