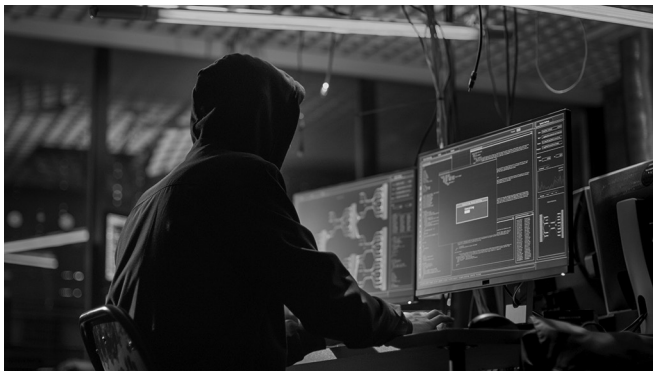
CENTRIWORKS

Ransomware Checklist



If you've ever been the victim of a ransomware attack you can probably identify with the cold sweats and the level of anger and frustration the insult produces in us.

In the perfect world you already have planned and practiced this scenario and know where the documentation is that is going to guide you through this trauma. Take a breath and let's figure out how to approach this injustice.

First, how many systems are infected? DON'T TURN THE COMPUTERS OFF, but do get them isolated and offline.

Now let's move through the plan we put in place. You'll be able to do this, because you'll have this *printed* checklist filed and ready to be executed.

If you don't have a plan in place, let us help you develop that plan. Our cybersecurity experts can develop a proactive strategy before hackers strike, and can help you work through the steps needed to recover from a ransomware attack.

1. ISOLATE THE INFECTED SYSTEM(S).
Do NOT power off the computer!!! Turning power off can destroy forensic evidence. Remove network access — unplug the computer from the network. Take the wireless access point offline.

2. CALL YOUR CYBERINSURANCE PROVIDER.
Answer their questions. They will guide you through the incident and help to ensure the correct procedure is followed. They are the experts; you are not the first to call.

3. DO NOT CONTACT OR COMMUNICATE WITH THE BAD GUY(S).
It may seem like a reasonable idea to talk with them, but it will just cause you more problems than it solves.

4. TAKE A PICTURE OF THE RANSOM NOTE ON THE SCREEN.
Having the picture insures you have information that the insurance company will want, and the incident handlers will need.

5. USE A CRISIS COMMUNICATION PLAN.
If you have not developed this, develop it. In a crisis you need to know who to call and who talks to outside entities, so things are communicated correctly.

6. TO PAY, OR NOT TO PAY? THAT IS THE QUESTION.
If network backups are unaffected and reasonably recent, that may be the way to go. Let incident response or cyberinsurance make the decision based on the facts of the incident.

©2020 CENTRIWORKS. ALL RIGHTS RESERVED.

7. HAVE A PRIORITY RESTORATION PLAN.
A business impact analysis is very helpful in letting you know which systems need to be restored first to get you back in business as soon as possible.

8. KNOW YOUR DATA AND THE ASSOCIATED REGULATIONS SURROUNDING THE DATA.
What kind of regulations are controlling the data and what are the reporting requirements?

- PHI (Personal Health Information) — HIPAA (Health Insurance Portability and Availability Act)
- Credit Card Info — PCI DSS (Payment Card Industry Data Security Standard)
- PII (Personally Identifiable Information) — This one is a doosy. Lots of laws may apply.
  - Consumer protection laws like the FTC Act (Federal Trade Commission Act).
  - Specific sectors may include laws like GLBA (Gramm—Leach—Blilley Act)
  - HIPAA
  - TCPA (Telephone Consumer Protection Act)
  - CAN—SPAM (Controlling the Assault of Non—Solicited Pornography and Marketing Act),
  - COPPA (Children's Online Privacy Protection Act)
  - FCRA (Fair Credit Reporting Act)
  - ECPA (Electronic Communications Privacy Act)
  - CFAA (Computer Fraud and Abuse Act)
  - State laws like CCPA (California Consumer Privacy Act)
  - EU (European Union) laws like GDPR (General Data Protection Regulation)

This is not an exhaustive list as nations and states enact new laws to control the exchange and processing of personal information and how it is defined.

9. DOCUMENT EVERYTHING!
Everything? Yes, as much as humanly possible. The cyberinsurance company is going to want to know and how they will pay, it is also how you can avoid something like this in the future.

EFFECTIVE CYBERSECURITY STARTS WITH A PROACTIVE STRATEGY.
If you find yourself needing help navigating things like this, please reach out to us, we can help. Since 1964, Centriworks has been East Tennessee's locally owned, nationally recognized business technology leader.

From identifying network security threats to data protection, web/email security and data encryption—we'll help you develop and implement the right solutions to keep your data safe, secure and private. We'll provide a cybersecurity program to deliver multi-layer protection, detect vulnerabilities, and protect your most critical business information.

We seek to identify potential threats that could be posed and take proactive measures of prevention, prioritizing security risks before they become a problem. Contact us today.

CENTRIWORKS

3505 Sutherland Avenue
Knoxville, Tennessee 37919
(865) 524-1124

4718 Lake Park Drive Suite 5
Johnson City, Tennessee 37615
(423) 283-0707

©2020 CENTRIWORKS. ALL RIGHTS RESERVED.