10-D Academy

IT Security • Compliance • Academy

*Setting a **Higher Level of Excellence** in Information Security & Compliance Services.*

Ransomware—What you Need to Know

Preparedness & Response Checklist:

Response Planning Actions

- ❑ Incident Response Plan (w/Communications)
- ❑ Cyber-insurance ("cyber extortion" coverage)
- ❑ Know how and where to obtain Bitcoin
  (Example: www.coinbase.com)
- ❑ Backups
  - ❑ Include ALL critical systems, securely.
  - ❑ Air gapped (i.e., off network) backups.
  - ❑ Maintain adequate retention period to mitigate against dormant malware.

Preventative Actions

- ❑ Require multi-factor authentication for remote access
- ❑ Training/Awareness
- ❑ Phishing/Spam filters
- ❑ Eliminate Local Administrator access
- ❑ Patch! Don't delay
- ❑ Disable macros in Word/Excel/PowerPoint/etc.
- ❑ Enforce Least Privilege Access
  (at minimum, set as "read-only")
- ❑ Advanced Antivirus – scan often
- ❑ Restrict and Detect scripting where possible:
  - ❑ PowerShell
  - ❑ HTML applications
  - ❑ PHP
  - ❑ VBScript
  - ❑ JavaScript
  - ❑ WSF & WSH
- ❑ Restrict access to file sharing & public email sites
- ❑ Intrusion Prevention System (IPS)
- ❑ Security log monitoring

Ransomware Immediate Response Actions

- ❑ Isolate the infected system (disconnect from network)
- ❑ Isolate or power-off other computers and devices to prevent infection
- ❑ Secure backups! Make certain that backup data is safe from attack
- ❑ Change all online and network passwords
- ❑ Contact cyber insurance carrier
- ❑ Contact local FBI field office, or FBI Internet Crime Complaint Center (IC3)

10-D, Inc.
10dacademyhelp@10dsecurity.com
www.10dacademy.com

(877) 208-5789 Toll Free

Keep your institution off the evening news. Contact us today!

8717 W 110th Street
Suite 500
Overland Park, KS 66210

Ransomware—What you Need to Know

Ransomware Resources:

Ransomware Self-Assessment Tool (R-SAT)

- Designed to identify gaps within an institution's current efforts to mitigate ransomware attacks
- Released by the Conference of State Bank Supervisors (CSBS) in collaboration with the Bankers Electronic Crimes Taskforce (BECTF), State Bank Regulators, & the United States Secret Service
- Can be used for any industry, though primarily for financial institutions
- Voluntary, though mandatory for financial institutions in some states

R-SAT can be found at:

https://www.csbs.org/ransomware-self-assessment-tool

Cybersecurity & Infrastructure Security Agency (CISA)

- In response to DarkSide ransomware attack, CISA released "Best Practices for Preventing Business Disruption from Ransomware Attacks":

https://us-cert.cisa.gov/ncas/alerts/aa21-131a

Get 10-Security's "Weekly Security Tip" at:

www.10dsecurity.com/weekly-security-tips.html