How to React After a Cyber Attack

CYBER SECURITY IS A MYTH AND CYBER ATTACKS ARE A REALITY. IT IS NOT IF YOU WILL BE ATTACKED BUT WHEN. HOW YOU RESPOND TO A CYBER EVENT WILL DETERMINE THE OUTCOME.

ATON Computing, Inc.

You can be protected, but never safe

- **Introduction**

  Implementing basic defenses is critical

- **IT priorities**

  Just get the network (data) back

- **Insurance influence**

  Mitigate liability & reduce costs

ATON Computing, Inc.

Be Proactive

- Develop an Information Security Management Plan
- In-house team (CERT)
- Cyber insurance
- Outsourced expertise
- SOPs & testing

ATON Computing, Inc.

You’ve been hacked!

- Contain the attack
- Assess the damage
- Recover from the attack
- Plan for the future

ATON Computing, Inc.

Contain the attack

- Contact the CERT team leader or Tech Support
- Isolate the infected computer from the Network
- Disconnect the network cable or
- Shutdown the wireless network connection or
- Last resort – turn-off the PC
- Contact Cyber Insurance hotline

Assess the damage

- Local computer issue only?
- Website access issues?
- Shared data unavailable – Ransomware?
- Network-wide security breach?
- Data theft?

ATON Computing, Inc.

Recovery steps

- Follow your Cyber Coach’s instructions
- Restore data from backups
- Repair/replace hardware/software
- Report incident to Law Enforcement authorities

ATON Computing, Inc.

Plan for the future

- Review the event
- Identify areas for improvement
- Implement upgrades
- Update the Response Plan

ATON Computing, Inc.

Case study - Ransomware

- Monday morning attack
- Immediate isolation of symptomatic PC
- Identified the scope of encryption
- The remediation process
- Four days later
- What we learned

Outside resources

- **United States Computer Emergency Readiness Team (US-CERT)**
  Collaboration groups and programs to facilitate information and resource sharing on cybersecurity issues
- **Multi-State Information Sharing and Analysis Center (MS-ISAC)**
  Cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial and tribal (SLTT) governments.
- **N.J. Cybersecurity & Communications Integration Cell (NJCCIC)**
  www.cyber.nj.gov is the State's one-stop shop for cybersecurity information sharing, threat analysis, and incident reporting.
- **National Institute of Standards and Technology (NIST)**
  Share best practices through the Federal Agency Security Practices.

Walt Contact information

ATON Computing, Inc.

Walter C. Hansen, CGCIO

PO Box 272, Somerville, NJ 08876

908-725-3700

walt@atoncomputing.com

www.atoncomputing.com

ATON Computing, Inc.