Cybersecurity for Companies in Receivership

Jenny Jeffers
Jennan Enterprises

Michael Morrissey
Morrissey Consultants

How are Failing Companies Different?

1. Insufficient IT Budgets
2. Staffing changes, usually at the top
3. Overpriced contracts
4. Eccentric or obsolete systems
5. Poor security that accommodates fraud
6. Angry employees and ex-employees

THREAT ENVIRONMENT

- Fraud and malicious acts
- Ransomware
- Intrusion and data theft
- Denial/interruption of service
- Reputation
- Others?

FIRST STEPS

- Interview management
- Administrative accounts – get logins, passwords, and ACLs for each application.
- Immediate backup of all key data, including email.
- Consider secure cloud storage repository

NEXT STEPS

SYSTEM INVENTORY - network diagrams, server and pc lists, firewalls, remote access etc.

DATA INVENTORY

- Policy holder data
- Claims data
- HR – Employee data
- Backups – what kind and where are they? Encrypted?

ASSESS LOGICAL SECURITY

- Deep dive – who has access to what?
- Password policies, multi-factor authentication
- Lock it down
- Disable old accounts

DATA ACQUISITION

Dealing with bad systems

- Bad design
- Historic merging of data
- Poor reporting functions

Data assessment – is it accurate?

- ACL and other tools
- Extraction
- Clean-up but preserve

RISK ASSESSMENTS

- **POLICIES & PROCEDURES** – Complete? Current?
- **VENDOR MANAGEMENT**
  - Colocation data center?
  - Hardware leasing?
  - Software licensing?
  - Partners sharing data?
  - Independent attestations (SOCs, etc.)

Source: Identitythefcenter.org

3rd Party Vulnerability Assessments & Pen Tests

- Consider the risk
- Timeline
- Remediation costs
- Other factors
- Incident Response Plans – a must!

IT Budget Review

- Is there a budget process in place?
- What can be cut?
- What security gaps must be filled?
- Outsourcing for security?
- Timeline?

Action: Restrict Sensitive Data

- ROLE BASED ACCESS – WHO AND WHY
- PASSWORD POLICIES
- ISOLATE SENSITIVE DATA
- CONTINUOUS MONITORING OF ACCESS

Action: Encrypt Sensitive Data

- “AT REST” ENCRYPTION – EFFECTIVE ?
- SERVERS
- LAPTOPS
- PORTABLE STORAGE DEVICES
- DATA IN TRANSIT
- CLOUD REPOSITORIES

Action: Monitor Systems and Data

- DATA CHANGES
- DATA LOCATION CHANGES
- ACCESS CHANGES
- SYSTEM CONFIGURATION CHANGES
- LOGS OF ACTIVITY – REVIEWED AND ARCHIVED

IPS/IDS systems can automate these

Incident Response Plan - Who you gonna call?

- What constitutes a security event?
- Steps to identify and assess a breach
- Seek professional help before hand
- Cyberinsurance ?
- Notification – the painful part
- Repair and learn

Questions & Comments ?

Jenny Jeffers
Jennan Enterprises, LLC

Michael Morrissey
Morrissey Consultants, LLC

Thank You.