Elements of a Cybersecurity/Information Security Plan

Presented By: Carter Schoenberg, President & CEO of HEMISPHERE Cyber Risk Management

www.hemispherecyber.com
(703) 881-7785
About HEMISPHERE

- Established in 2015
- Offices in U.S. (Virginia) and Panama
- Professional cyber risk management services
  (Small & Mid-size Businesses, Law Firms, and Insurance Sectors)
- Proprietary risk modeling
What is a Cybersecurity Plan?

An operational capability to effectively respond and recover from a cyber event that negatively impacts your business operations.
Who needs a Cybersecurity Plan?

My business is too small to worry about this, right?
Did You Know?

- 60% of small businesses close their doors after a cyber event.
- Most cyber events are internal.
- More money is spent on cyber defense today than ever before.

~ Small Business Trends, 2017
Did You Know?

- 62% of all cyber insurance claims came from small businesses
- Most coverages levels are inadequate
- Duty to disclose before taking action
- Courts are moving away from “if you were breached” to “how well did you respond and recover?”
Risk Assessment – Where to Start?

What system and data resources are you responsible for?

Data Types to Consider

**Personnel**
- 401
- Social Security Numbers
- Addresses
- DOB
- Personal email
- Telephone numbers
- Fitbit/ health challenges

**Client or Business Partner**
- Credit Card/ Banking Information (ACH)
- EHR
- Proprietary data
- Mailing lists
- PII
Do you know what regulatory requirements apply?
- HIPAA
- PCI

What about....
- State Data Breach Notification Law(s)
- DFAR/CUI
- FTC
- NYDFS Cyber Law (Aug -2017)
- GDPR
Understand the threat landscape

- Individual Actors
- Nation State
- Organized Criminal Syndicate
Risk Assessment Done – Now What?

- Create corporate-security policies and make sure all employees commit to them.
- Create an incident response plan.
- Train employees in key areas – acceptable use, password policies, defenses against social engineering, and avoiding phishing attacks.
- Encrypt all records and confidential data to be more secure from cyber attack.
- Perform frequent backups and keep a copy of recent backup data off premises.
Cyber Plan vs. SSP

Some entities require a System Security Plan (SSP). How is a SSP different from a “Cyber Plan”?

Context and Visualization

<table>
<thead>
<tr>
<th>AG.1 Access Control Policy and Procedures</th>
<th>Adopted (X)</th>
<th>Not Adopted ( )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments: ACME has three organizations (Police, Fire and Paramedic). The initial assessment supports that technical controls are well established but to date, there is not one unified governance document to ensure consistency and adherence to mutually agreed upon best practices. As identified in the assessment, some presumptions about device configurations and network paths were refuted. Physical access to critical ACME computing assets are protected by key access controls in server rooms in multiple locations. In instances where assets are co-located, there are physical barriers under lock and key.</td>
<td>Adopted with limitations (X )</td>
<td>Not Adopted ( )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AG.2 Account Management</th>
<th>Adopted (X)</th>
<th>Not Adopted ( )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments: ACME has assigned account managers for information system accounts. Conditions for group and role membership is specified by the equipment manufacturer and warrants consideration as to how to better define unique identifiers tied to specific users for “Admin” and “Super Admin.”</td>
<td>Adopted with limitations (X )</td>
<td>Not Adopted ( )</td>
</tr>
</tbody>
</table>

While approvals for access appear to be in place, it is ad hoc and aligns with the gap described in AC.1 where approvals for access should be structured and standardized thereby limiting ambiguity in the face of why a ACME employee was granted access to the system and/or access is revoked due to the employee’s role or operational status (transferred, fired, resignation, etc.).

A process or technical capability for monitoring activity (by account) is not enabled.

## 1.1 ACCESS ENFORCEMENT

Automated Rules of Behavior (ROB) are implemented in [Company Name Here]. There are two different ROB:

1. Privileged: Users with DB or Admin role
2. Non-Privileged or (Basic): Users without DB or Admin role who are not employees. This includes (Business Associates here if applicable).

Privileged Users will be presented the ROB for Users with Privileged Access to Information Systems. Non-Privileged Users are required to select the appropriate ROB at first login per database prior to receiving access to the application. If a user elects to decline the ROB, access to [Company Name Here] will not be granted.

In addition, agency security awareness training must be renewed annually by all Federal Agency users in accordance with their Agency policy. Other [Company Name Here] access enforcement features are provided by the application, which includes:

- [Password syntax and character set rules](#)
- [One User ID/password combination per user](#)
- [Passwords that expire every 60 days](#)
- [Password history](#)
- [Locked user accounts after five consecutive failed login attempts](#)

### 2.1.1 Password Syntax and Character Set Rules

[Company Name Here]. passwords must be between 10 to 20 characters in length and may consist of upper or lower case letters, numbers, and/or special characters as follows:

- Minimum of one capital letter
- Minimum of one lower case letter
I don’t have time for this stuff!

There are lots of free templates out there (DHS/FTC, Other)

**Issues**

- Presumes you know how to complete
- Can be very resources intensive.
Corporate Security Policies and Incident Response Plan

It is not simply “your” Business you need to worry about.

63% of cyber breaches attributed to a 3rd party.
~ Soha Security Survey 2016
Corporate Security Policies and Incident Response Plan

What will be asked for?

Likely first items

- Corporate Policies
- Incident Response Plan
Corporate Security Policies and Incident Response Plan

What to Do

- Make it easily accessible
- Actionable
- Repeatable

What Not to Do

- Paper version stuck on a shelf
- Very technical
- Hard to enforce
Cyber Plans in Place – Now what?

Assess the plan’s functionality

- Compare policy to operations
- Who attended? Was it documented?
- Did the plan operate as intended?
- Was a gap identified between the IR Plan and the authority of what was within the corporate policies and procedures? (If so, revise documentation to apply lessons learned)
Test both escalation paths
Questions

For a free demo on HEMISPHERE’s cyber plan program, email us at contact@hemispherecyber.com  SUBJECT: GENEDGE

H.A.C.K.E.R Training
- Video Tutorials (Access Control, Media Protection, Legal Considerations, Incident Response)
- Structured Templates for rapid implementation

Pre-event and Post-event cyber risk services

Carter Schoenberg, President & CEO
Carter@hemispherecyber.com
(703) 881-7785 Office