Cybersecurity Risk Management

ANDREW BROCK, BLUE & CO.

TOM SKOOG, BLUE & CO.
Cybersecurity Trends

Tom Skoog, Cybersecurity & Data Management Practice Leader
Meet the Team

Tom Skoog
Cybersecurity & Data Management Practice Leader
Principal

Andrew Brock, CPA
Not-For-Profit Audit Senior Manager
Agenda

• Impacts of Ransomware on Grantmaking Organizations
• Drastic changes in the cyber insurance industry
• Assessing Risks and Implementing Controls
Impacts of Ransomware on Grantmaking Organizations

Number of “reported” ransomware attacks first 6 months of 2021

Downtime Cost – first 6 months of 2021. $419M total cost for 2020

Increase in individual ransom demands

2084

$590

71%
Changes in Cyber Insurance

**IN 2021:**

- **Increasing premiums** 30 to 40 percent for small business to 300% for high-risk industries (e.g., Healthcare, Law)
- **Increasing retentions** connected to revenue
- **Decreasing capacity** maximum limit $5M
- **Carriers exiting market**
- **Changing underwriting appetite** more high-risk industry verticals
Changes in Cyber Insurance

BASELINE CONTROLS EXPECTED IN THE CYBER INSURANCE APPLICATION PROCESS

- Multi-Factor Authentication (MFA)
- Network segmentation
- Data backups
- Disabled admin privileges
- Training and awareness
- Anti-Virus/Malware Software
- Strong passwords
- Sender Policy Framework
- Endpoint Detection and Response (EDR)
- SOC and SIEM
Assessing Risks and Implementing Controls
Assessing your Business’s Risks and Vulnerabilities

- **Identify**
  - What is confidential
  - How important is data integrity
  - What if our systems were unavailable

- **Source**
  - What can compromise confidentiality, integrity, availability

- **Measure**
  - Assess your current state

---

<table>
<thead>
<tr>
<th>Probability</th>
<th>Definition</th>
<th>Impact</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probable</td>
<td>Risk will occur</td>
<td>Intolerable</td>
<td>Critical effect</td>
</tr>
<tr>
<td>Possible</td>
<td>Risk likely to occur</td>
<td>Tolerable</td>
<td>Moderate effect</td>
</tr>
<tr>
<td>Improbable</td>
<td>Risk unlikely to occur</td>
<td>Low</td>
<td>Little to no effect</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Probability</th>
<th>Acceptable</th>
<th>Tolerable</th>
<th>Intolerable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improbable</td>
<td>Low</td>
<td>Low</td>
<td>Med</td>
</tr>
<tr>
<td>Possible</td>
<td>Low</td>
<td>Med</td>
<td>High</td>
</tr>
<tr>
<td>Probable</td>
<td>Med</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
Security Frameworks & Practical Considerations

NIST CYBERSECURITY FRAMEWORK

RECOVER
IDENTIFY
PROTECT
RESPOND
DETECT

CYBERSECURITY FRAMEWORK VERSION 1.1
Security Frameworks & Practical Considerations

FOR YOUR ORGANIZATION

• Stay Current with Technology
• Patching
• Train
• Strong Passwords & Encryption
• Back up Data
• Anti Virus/Malware
• Look for Monitoring Help
• Incident Response Plan
• Get Insured
• Rely on your Experts
Conclusion

- Grantmaking organizations are not immune from cyber attacks or ransomware
- The cyber insurance market has dramatically changed in 2021 (and not for the better)
- If you have questions of where to start, there are various cybersecurity frameworks (standards) which act as a “playbook”
Contact Me

Tom Skoog
Cybersecurity & Data Management Practice Leader
Principal

Email: tskoog@blueandco.com
Phone: 614-220-4131
Feeling inspired?

PLEASE RATE THIS SESSION BEFORE LEAVING