Cyber Incident Response Plans for Nonprofits (Live Q&A)

Presented by

Dave Kelly
Co-Founder/CTO, SensCy

Leda Muller
Founder/CEO, Pocket Security

Host
Julie Bernhard
Agenda

• What a cyber incident response plan is

• Why your nonprofit should have one

• What should be included
Ransomware attacks – average 16.2 days of downtime in 2022 - IBM
All efficient and successful responses to cyberattacks started long before the incident occurred!
What is a Cyber Incident Response Plan

A Written Guide
- Before an Incident
- During an Incident
- After an Incident

A roadmap of actions and responsibilities necessary to ensure an organization can recover as efficiently as possible from a cyberattack.

A Component of
- Business Continuity Plan
- Disaster Recovery Plan
Poll Question 1

Does your nonprofit have a Cyber Incident Response Plan specifically designed for cybersecurity incidents?
### Efficient Response = Efficient Recovery

- Reduces business disruption
- Reduces reputational risk with clients
- Builds trust with partners, supply chain, and employees

### Engaged Leadership = Efficient Response

- Nonprofit leaders must be involved in development
- Key personnel must be assigned in advance and know their roles
- Authority must be given for early decisions

---

**43% of cyberattacks now target small businesses - Fundera**

**SensCy has surveyed over 200 SMO’s and 66% of them do not have an ICP**
What Should be Included in a Cyber Incident Response Plan?
### The Incident
- Are we keeping logs?
- What kind of attack is this (ransomware, unauthorized access, DDoS, Malicious Code, etc.)?
- What systems are being impacted?
- How is it disrupting the business & what stakeholders are impacted?
- When was the incident first reported, and who reported it?
- Who do we need to notify?

### The Recovery
- Where was the vulnerability that caused this incident?
- How widespread was the damage?
- What are the recovery steps?
- Are we documenting all recovery steps and expenses incurred?

### After-Action
- What mitigation measures were instituted to prevent a recurrence?
- Any required new policies, procedures or technologies?
- Response & remediation – what worked/didn’t work?
- Communication recommendations?
- Financial or budget recommendations/changes?
Predetermined Alternative Communication Methods

- Set up text message group with all key members cell phone numbers
- Establish free Gmail accounts and notify key stakeholders via SMS
- Use and end-to-end encrypted messaging app like Signal – ask team members to download the app on their mobile device
<table>
<thead>
<tr>
<th>Potentially Impacted Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees</td>
</tr>
<tr>
<td>Customers</td>
</tr>
<tr>
<td>Partners</td>
</tr>
<tr>
<td>Vendors</td>
</tr>
<tr>
<td>Supply Chain</td>
</tr>
<tr>
<td>Investors</td>
</tr>
</tbody>
</table>
Are you interested in getting your free, no-obligation SensCy Score?
THANK YOU