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

Sponsored by

SENSCY
Your Trusted Guide to Sensible Cyber

Agenda

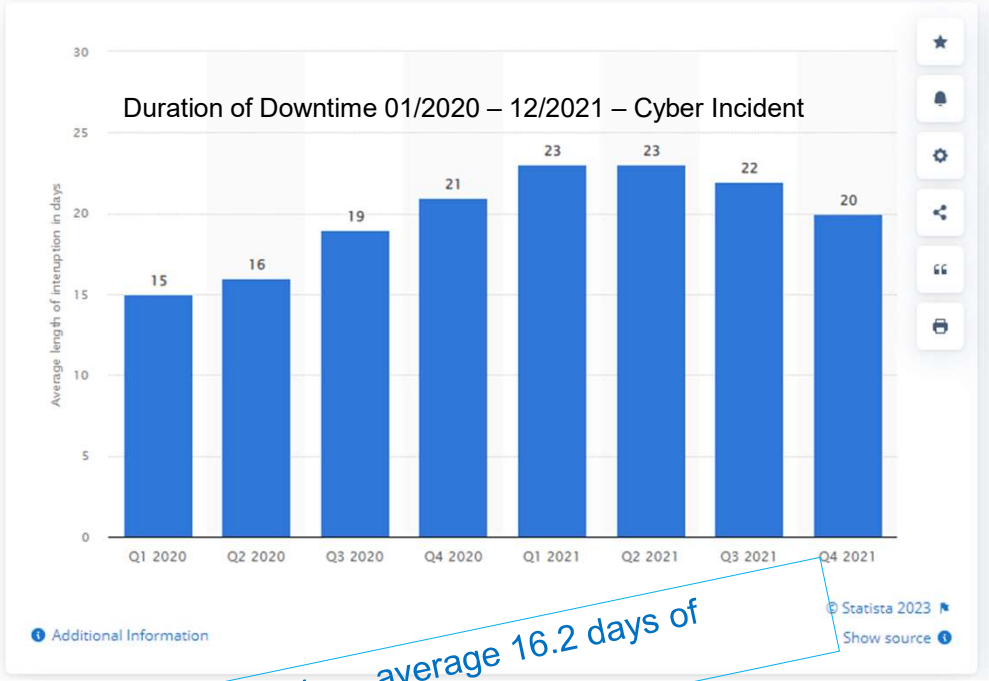
- What a cyber incident response plan is
- Why your nonprofit should have one
- What should be included

Dave Kelly
Co-Founder/CTO
SensCy

Leda Muller
Founder/CEO
Pocket Security

POCKET SECURITY

Cyber Incidents = Business Disruption



Ransomware attacks – average 16.2 days of downtime in 2022 - IBM

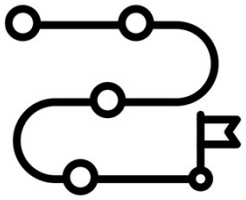
Now What?

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

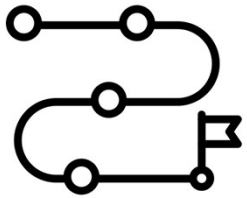


A roadmap of actions and responsibilities necessary to ensure an organization can recover as efficiently as possible from a cyberattack.

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?

Why is a Cyber Incident Response Plan Important?

Efficient Response = Efficient Recovery	Engaged Leadership = Efficient Response
• Reduces business disruption • Reduces reputational risk with clients • Builds trust with partners, supply chain, and employees	• 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?

Guidance on Asking the Right Questions

Empower Nonprofit Leaders

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?

blue avocado

Internal Communications – How will we manage this crisis?

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

External Communications – What do we say?

Potentially Impacted Stakeholders

- Employees
- Customers
- Partners
- Vendors
- Supply Chain
- Investors

SENSCY
Your Trusted Guide to Sensible Cyber

CONFIDENTIAL – FOR INTERNAL USE ONLY – DO NOT SHARE

SAMPLE EXTERNAL COMMUNICATION

NOTE: External communications should be reviewed by your legal team

DATE _____

Dear _____

This letter is to inform you of a cybersecurity incident that impacted (list what was impacted). This incident resulted in your data being compromised by an outside entity. Our Cybersecurity Incident Response Team acted quickly to assess and mitigate the situation.

Currently, we can share the following details:

[List a brief description of the breach, the date of the incident, the date of discovery; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the investigation, plan to investigate, and remediation steps taken]

Please know that (list company name) remains committed to protecting and securing your data. Our team has extensive training in data security and privacy, and our systems have many controls in place to protect your data. We are working with a group of external experts to review the incident and implement appropriate measures to protect against this type of incident from occurring in the future.

Please contact (name of person identified by the executive team to discuss this incident) with any questions you may have regarding this incident and our response.

Sincerely,

blue® avocado

What is Your

SensCy Score™?

SENSCY™

Your Trusted Guide to Sensible Cyber

Are you interested in getting your free, no-obligation SensCy Score?

blue® avocado

SENSCY®

Your Trusted Guide to Sensible Cyber

THANK YOU

Dave Kelly

Co-Founder/CTO
SensCy

Leda Muller

Founder/CEO
Pocket Security

POCKET SECURITY