nten

CONNECT ▸ LEARN ▸ CHANGE

Cybersecurity for Nonprofits

Critical Questions

Written by Afua Bruce

February 2020

How Do We Measure Cybersecurity Planning Success?

After taking the time to develop and implement a cybersecurity plan, organizations must ask themselves: "How do we measure success?" Training employees, conducting risk assessments, and purchasing protective software or insurance, all require a significant investment of time and money. The easiest questions to ask may be "Did we fall victim to a cyberattack?" and "Did we recover from any and all cyberattacks?" But, to effectively monitor cybersecurity preparedness, more nuanced questions are required. Organizations should define Key Performance Indications (KPIs) specifically for cybersecurity activities.

Any process of defining KPIs requires organizations to thoughtfully consider what to measure and why it matters. For cybersecurity KPIs, this means understanding the business context, identifying audiences and collaborators, determining common interests, and identifying the key information security priorities.

The first step to defining cybersecurity KPIs is to think through the different elements of an organization's cybersecurity plan and identify key implementation outcomes. Then, organizations must translate the key outcomes into measurable statements and set targets. An example of this process on implementing cybersecurity for training employees appears below.

Category	Goal	Measure/KPI	Target
Training Employees	Employees are trained	Percentage of employees who completed cybersecurity training	90%
		Average score on cybersecurity training test	90%
	Employees securely access the internet	Percentage of employees who use a VPN	70%

[1] Olavsrud, Thor. How to Measure Cybersecurity Effectiveness – Before It's Too Late. https://www.cio.com/article/3221426/how-to-measure-cybersecurity-effectiveness-before-it-s-too-late.html Aug. 31, 2017.

In the training category specifically, some organizations will even create applied methods to test their employees understanding of cybersecurity principles. For example, IT departments will send out fake phishing emails, and track how many employees fall victim to the social engineering technique.

Additional categories to create KPIs for and example associated metrics include:

- Access Control (Number of people with “super user” access, number of days to deactivate former employee and volunteer accounts, number of times organizational passwords are changed)
- Baselines (how frequently backups are done, number of information sources backed up)
- Security Policy/Compliance Adherence (patching levels, time between patch release and installation, firewall data)
- Monitoring and Response (Number of cybersecurity incidents, Number of cybersecurity incidents reported by employees, Mean-time-to-respond, Percent of incidents responded to within organization-defined amount of time)

If an organization takes advantage of third parties to provide any aspect of its cybersecurity plan, the organization should regularly ask for performance indicators. Similarly, if an organization has cyber insurance or relies on another entity to respond to cybersecurity incidents, the organization should regularly confirm the notification and response terms of the agreement.

Just as cybersecurity plans may scale based on the size, complexity, and vulnerability of an organization, cybersecurity metrics and KPIs may also scale based on the same factors. Organizations should set a number of metrics that can be measured within the organization’s structure, and can be regularly reviewed by both IT and executive leadership. Tracking metrics over time will give organizations an understanding of how effective their cybersecurity plan is and point to areas that require additional focus.

[2] Cipher, a PROSEGUR company. 10 Cybersecurity Metrics You Should Be Monitoring. https://cipher.com/blog/10-cybersecurity-metrics-you-should-be-monitoring/

[3] Zhang, Ellen. Security and Analytics Experts Share the Most Important Cybersecurity Metrics and KPIs. https://digitalguardian.com/blog/what-are-the-most-important-cybersecurity-metrics-kpis Dec. 8, 2017.

What Do We Do After a Cybersecurity Incident?

Even after creating a cybersecurity plan, training employees, and implementing security protocols, organizations may still fall victim to a cybersecurity attack. How should organizations respond after attacks? What should be done after initially – and hopefully quickly – moving through the initial shock of realizing that systems have been compromised?

A critical element to effectively responding to a cybersecurity attack is a clear understanding of who needs to be involved with the response. Organizations should adopt a "stay ready so you don't have to get ready" mindset to this. Pre-determine who in the organization immediately needs to be notified of a security breach; that is, who on the IT team will need to involved, when executive leadership will need to be notified, and who specifically on the executive leadership team will make decisions about the broader communications. If applicable, also pre-determine how to engage the cyber insurance company or third-party application provider if a cybersecurity attack affects their systems. Organizations should also determine when and what will be done regarding access to data. Will systems be immediately taken offline, or will passwords simply be changed, or will some other action be taken? Organizations should also maintain continuity plans so they can continue to operate if a website or portion of their network is taken offline. This is good practice even without the threat of cybersecurity attacks!

After identifying a cybersecurity attack, organizations should follow these steps:

1. **Activate the Response Team.** The predetermined individuals tasked with responding to and making decisions about cybersecurity incidents should quickly assemble. In addition to IT and executive leadership, organizations should invite legal counsel to participate in discussions. Of course, if organizations have cyber insurance or third parties to manage cyber security, representatives from those organizations should help lead the response.

2. **Secure Systems.** As soon as an attack has been detected, the organization's goal should be to contain the attack and prevent further harm. Begin by changing passwords, prioritizing admin passwords on affected systems. Organizations may need to isolate and suspend portions of their IT network. Note that simply removing malware may not be enough to stop an attack.

3. **Restore Backups.** Once the attack has been contained, infected software removed, and hackers no longer have access to the system, organizations should begin repairing the system. One way to do this is to restore backups of the last point in time when an organization's systems were secure.

4. **Investigate.** Organizations should determine how the hackers gain access to the system. In a worst-case scenario, an organization may need to take HR action against an employee involved in the breech. The result of the investigation will drive changes to the organization's cybersecurity plan.

5. **Communicate Externally.** Depending on what data was compromised, people external to the organization must be notified. There are legal and regulatory reporting requirements for some data breeches. Organizations may want to alert law enforcement for cybersecurity attacks – both to report the crime and for possible assistance to determine who executed the attack. Finally, if Personally Identifiable Information was compromised, or users were subjected to scam communications, organizations should notify their clients, volunteers, and donors.

While organizations must start by activating their response team, steps 2-5 do not have to be done sequentially; rather, organizations should think of doing multiple steps concurrently.

It is important to remember that with the rise in the number of cybersecurity attacks, "most organizations will be judged on how they respond to an attack, versus the fact that they were attacked in the first place." Organizations, therefore, must proactively address the concerns of relevant stakeholders throughout the response, noting, of course, that the definition of "relevant" will change with the size and scope of the cybersecurity incident. Often, responses to cybersecurity attacks have a long tail; the attack may be quickly contained, but the recovery and communication can last significantly longer. With proper preparation, the ability to dedicate sufficient resources in the response, and a fair amount of tenacity and patience, organizations can recover from cybersecurity attacks.

[5] Rossi, Ben. Six Critical Steps for Responding to a Cyber Attack. https://www.information-age.com/6-critical-steps-responding-cyber-attack-123459644/ June 11, 2015.

[6] Perlman, Al. The Dos and Don'ts of Responding to a Cybersecurity Attack. https://www.securityroundtable.org/the-dos-and-donts-of-responding-to-a-cyberattack/ Nov. 8, 2018.

[7] Deloitte. Cyber Crisis Management: Readiness, Response, and Recovery. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf 2016.

nten

CONNECT ▸ LEARN ▸ CHANGE

NTEN envisions a just and engaged world where all nonprofits use technology skillfully and confidently to meet community needs and fulfill their missions. We support organizations by convening the nonprofit community, offering professional credentials and training, and facilitating community skill and resource sharing.

NTEN reports support the growth and development of the sector through benchmarking the technology goals and challenges of nonprofits, and identifying areas of need. For more, visit **nten.org/reports**.

Microsoft

Microsoft's Tech for Social Impact program empowers nonprofits and humanitarian organizations around the world with technology to advance their missions.

With recognition that many nonprofits have limited IT staff, the program provides solutions and resources that help nonprofits innovate new ways to tackle global issues. For more, visit **microsoft.com/nonprofits.**