A Nonprofit Quick Start Guide to Building Cybersecurity Incident Response

First Edition
October 2023

Information Technology
Outreach and Education Program

Questions about this guide or TechOE program services contact:

Kai Dailey Program Manager
Information Technology Outreach and Education Program
501 Commons
kai@501commons.org

Building a comprehensive cybersecurity program even in a small organization is a long-term, complex undertaking that cannot be fully outsourced.

If you want to get started quickly, first build an incident response team (IR Team). The effort can bring tremendous on-going value to the organization and provide a quick return on investment in the event of an incident. A dedicated IR Team creates peace of mind and provides in-house incident response leadership during a crisis. A well-structured team that meets regularly can provide the following functions:

- provide cross-functional security oversight;
- source external security assistance;
- draft a response plan;
- assist with selecting security priorities that align with business goals;
- make policy recommendations to executive leadership and board members; and
- provide training and security advocacy throughout the organization.

The biggest myth about cybersecurity is that it is a field limited only to technical specialists.

As you will discover when building a security program, technical specialty is one of many important areas within the wider cybersecurity field. In small organizations, non-technical staff can and must participate in monitoring and securing cloud applications, inventorying and stewarding data appropriately, and consistently practicing cybersecurity hygiene.

Another common and inhibiting myth is that cybersecurity is so high-risk and fraught with liability issues that all aspects of a security program must be left to experts.

The truth of this runs along a continuum. There are organizations with highly complex IT infrastructure and legally regulated data collection and storage, and there are also small five-person organizations who operate entirely in the cloud and maintain a mailing list in MailChimp.

Functionally, the continuum is no different in our personal lives. Each of us should be taking steps to secure the applications, devices, and information we store and use. Whether or not we hire a cybersecurity contractor to secure our home networks will depend on the same factors mentioned above: the technical complexity of our information systems and the type and value of data collected, stored, and used.

It is essential to develop a detailed knowledge of the information your organization collects, uses, and stores.

You must identify what data are most valuable to your organization and also develop an understanding of what information is most valuable to potential thieves. You will need to document where high value data are stored, who uses it, and how it is used. With this information, the business aspects of cybersecurity become understandable as an exercise in reducing risk. All security efforts can then be guided by the goals of (1) protecting your most valuable hardware, software, and data assets and (2) eliminating or reducing vulnerabilities that could allow a compromise in one system, for example, a laptop, to spread to your email server or to a government database your organization accesses.

Admittedly, this process takes time, even as cyber threats are ever present and increasing. According to the federal agency Cybersecurity & Infrastructure Security Agency (CISA), cybersecurity attacks increased 40% globally in 2022 over the previous year. Assume that your organization will experience a cybersecurity incident, hopefully it will be a minor one.

For a Quick Start

—Create an incident response team (IR Team)

—Empower the IR Team to create a basic response plan (IR Playbook)

—Put essential cybersecurity measures in place (backups, MFA, device encryption, etc.) with project oversight by the IR Team

—Train all staff and executive leadership and any volunteers and contractors who access your computer networks and information on general cyber safety

—For staff members, make training participation and the consistent practice of cyber hygiene an annual performance evaluation standard.

Once the IR Team structure is completed, the team can begin rehearsing incident scenarios that may be likely for your organization. For example,

—a lost or stolen device (cell phone, laptop, or USB hard drive) with legally protected data

—a hijacked cloud software account

—a data storage account or server held for ransom

—legally protected information discovered on the dark web, requiring data breach notification to federal or state entities

—sensitive information leaked to the media

—email server compromise.

As the IR Team works through these scary scenarios, they will begin to see how most scenarios require both a technical response and a business response, and possibly legal, law enforcement, or an external cybersecurity forensics team.

Why start with incident response?

Shouldn't the focus be on defending against cyber-attacks and increasing security measures? If you have an active security program in place but do not have a formal incident response structure, then developing an incident response plan is an essential next step toward maturing your cybersecurity program.

If you are at the beginning of security development—which means you may be without basics like multi-factor authentication (MFA), consistent backups of essential data, or regular phishing email training and

testing—creating an IR Team can help your organization implement these security measures and prepare to respond to the unexpected.

With limited resources for cybersecurity, it is essential to leverage the assistance that a dedicated and well-organized team can provide. Together they can work to bring cybersecurity into the daily workflows of your organization and empower all staff members. By using a whole-organization approach, it is possible to do more with less and improve your security posture.

Keep these tips in mind when developing your IR Team and program

In the selection of IR Team members, good interpersonal and communication skills and the ability to work calmly under pressure should be regarded as equal in importance to technical or business expertise and experience.

Train often as a team. Be the calm during a crisis. The IR Team must slow the response process down to allow for a thorough investigation to determine the nature of an event and whether it should be treated as an incident.

There will be trial and error involved when developing roles and determining what roles should handle which tasks during an incident. Rehearsal is essential to discover process and communication issues within the team. The hierarchy of the IR Team supersedes your organizational hierarchy during an emergency. Normal job titles should be superseded by the IR Team role.

If it's not written down, you cannot categorize it as implemented. In the event of a serious data breach, written policies become important to the response process, essential during a lessons learned review, and potential evidence in the case of legal proceedings that result from a serious data breach.

Incident Response Toolkit

A Nonprofit Quick Start Guide to Building Cybersecurity Incident Response (First Edition)

This handout (the document you are now reading) by 501 Commons is written for small and medium-sized nonprofits. It advocates for the creation of an incident response team as a first step toward building a cybersecurity program. The guide includes a curated list of free resources to support building an IR Team.

Computer Security Incident Handling Guide

NIST SP 800-61 is a publication from the National Institute of Standards and Technology (NIST). It provides guidelines and detailed steps for developing and implementing a comprehensive incident response program. It covers the entire incident response lifecycle, from preparation and detection to post-incident activities and lessons learned.

Based on the NIST Cybersecurity Framework, it is a vendor-neutral guide that both technical and non-technical readers can use as a go-to reference throughout the entire incident response development process.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Building an Information Security Awareness and Training Program

NIST Special Publication 800-50 provides guidelines and best practices for developing and implementing an information security awareness and training program. Small organizations can find a lot of inspiration in this comprehensive, federal agency-focused publication. From sources of awareness training materials to lists of awareness topics (Pgs. 24-25), it's a vendor-neutral reference that you can keep returning to as you build and grow your program.

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf

Microsoft's Incident Response Reference Guide

This guide is focused on the Respond and Recover phases defined in the NIST cybersecurity framework. This well-organized, easy to read PDF, addresses both technical and business response.

Technical readers will find details about malware analysis and host recovery procedures. Non-technical readers may find jargon like "HVAs" (high-value assets) and "C2 channels" (command and control channels) unfamiliar. Read this for the specific dos and don'ts, tips, and critical success factors detailed for each phase.

https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf

AT&T's Insider's Guide to Incident Response

This web booklet is an excellent beginner's resource on setting up an IR Team. Well-written and visually appealing.

https://cybersecurity.att.com/resource-center/ebook/insider-guide-to-incident-response

Cybersecurity Awareness Assessment Tools

Awareness training is important to incident response planning because it helps staff identify and report security incidents quickly. When staff are aware of the latest threats and vulnerabilities, they can take steps to protect themselves and the organization from attack.

Cybersecurity awareness training also helps staff to understand their role in the incident response process. For example, staff may be responsible for reporting suspicious activity, isolating infected devices, or backing up data. By understanding their roles and responsibilities, staff members can help to minimize the impact of a security incident.

Cybersecurity awareness training can support:

- Reduced risk of data breaches
- Faster detection of security incidents
- Improved response effectiveness
- Promote a shared security language and ethic

Who should receive training?

Anyone with access to your information systems should get training:

- Staff
- Contractors
- Volunteers
- Board members
- IT

While cybersecurity awareness training is a must-have, using an awareness framework to assess "cybersecurity awareness maturity" is a nice-to-have. However, a maturity framework can assist you with informal, qualitative efforts to identify areas for improvement, manage organizational change, and improve employee morale. A framework can be helpful for identifying and interpreting common indicators of low awareness and recognizing indicators of improvement.

There are a number of different maturity models available. The SANS Security Awareness Maturity Model is a researched framework developed by a respected for-profit cybersecurity training organization. SANS provides certifications and advanced training for cybersecurity professionals. Their professional development courses are quite pricey. However, they have made their framework tools and some learning content available for free.

Free leadership training and security awareness content
https://www.sans.org/cybersecurity-leadership/

SANS Security Awareness Planning Toolkit
https://go.sans.org/lp-kit-security-awareness-planning

SANS Security Awareness Roadmap
https://sansorg.egnyte.com/dl/zLpElKi24l