Cybersecurity Standards of Care 101

Prioritizing Risk Management

Business Executives for National Security

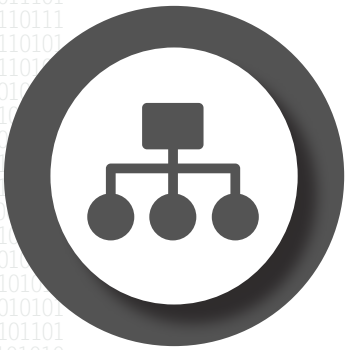
Cybersecurity risks threaten all organizations and corresponding stakeholders; they are increasingly frequent and sophisticated, posing a threat not only to our economy but also to our national security. In response, the White House released its comprehensive cyber strategy in 2018. The Framework for Improving Critical Infrastructure Cybersecurity also was most recently updated in 2018 by the National Institute of Standards and Technology (NIST)[1]. The Department of Homeland Security (DHS), the lead civilian hub for cybersecurity and infrastructure protection risk management, recently elevated the National Protection and Programs Directorate into a full-fledged component agency, the Cybersecurity and Infrastructure Security Agency. These developments, strategies, and capacity building frameworks collectively outline how the U.S. government intends to prepare, protect, and defend the nation from cyber adversaries.

In this context, organizations, large and small, public and private, should be aware of the threat environment and have a resilient plan in place to prevent the spread of problems and minimize business disruption. Standards of care and response best practices apply universally. For these reasons, an organization's top leaders should consider implementing basic risk management practices in preparation for a cybersecurity event.

[1] More information on NIST's Framework for Improving Critical Infrastructure Cybersecurity is available at https://www.nist.gov/cyberframework

Steps to take **inside** your organization...

01



Designate roles at the board and senior management levels with defined responsibilities for reporting structure and accountability. Develop a clear set of decision-making protocols and establish individuals and teams to deal with particular responsibilities.

Assign team roles and responsibilities, such as:

- Management/board oversight and responsibility;
- Technical incident response team;
- Timely internal and external communications.

Establish decision matrix and rights:

- Identify who decides when;
- Identify threshold criteria for taking decisions.

02

Identify crises management team and associated processes, including scope of responsibility and reporting structures.

Establish a crisis management team (CMT):

- Define policies and procedures that guide the CMT response;
- Assign responsibilities to individuals and provide appropriate training;
- Include operations experts as well as traditional IT experts.

Establish a cybersecurity incident response testing process including test plans, actions and test scenarios to improve incident detection and response:

- Per industry standard, tests should be conducted at least annually and when warranted by organizational business environment change;
- Establish quantitative and qualitative metrics for the incident response process;
- Formalize information flows.

Develop emergency preparedness and crisis management plans that include an accurate contact tree, as well as primary and emergency contact information for communicating with employees, service providers, vendors, law enforcement, regulators, municipal authorities, emergency response personnel and media.

Exercises and Training: Test plans for continued readiness and continuous improvement:

03

Establish organizational, departmental, and role-based information security training (use off the shelf training tools to train staff how to identify various attack techniques);

Regularly update security policy with requirements for training during onboarding and at periodic intervals during period of employment;

Regularly exercise and plan (live exercises are best): penetration tests, table tops, red teams, white hat data breech exercises.

IT Hygiene: Design network with trusted users, devices, and applications capable of combating actors pursuing illicit aims using licit and illicit means. Rely on automated data-centric and user-centric strategies and processes aligned with your organization's established security protocols. Hygiene should extend to devices not connected through hardware to the system (such as phones, tablets, printers/copiers).

04

Identify users – who is connected to your network and what privileges they have (especially administrators):

- » Implement and adapt specific user restrictions and permissions for discrete access to the network;
- » Implement multi-factor user authentication and user log management protocols.

Identify your devices – what hardware is connected to your network:

- » Inspect all hardware on arrival and before usage;

- » Verify the identification of all devices interacting with networks and systems;
- » Ensure alignment of old and new infrastructure and systems;
- » Hygiene should extend to devices not connected through hardware to the system (such as phones, tablets) and prohibitions or conditions on use of WiFi distant from office locations.

Identify and secure your applications – what software and processes are running on your network:

- » Inspect all applications permitted for use;
- » Ensure common standards for enterprise to enterprise secure digital identity of both institutions and empowered individuals within those institutions;
- » Define a security strategy in your organization's software development activities.
- » Establish automated systems to alert regarding patches/updates and confirm implementation for all users/devices/applications on your network;
- » Identify and isolate unprotected systems on your network.

Implement data redundancy measures:

- » Provide cloud or non-accessible off-site data back-up to on premises databases;
- » Categorize data assets to allow for a risk-based approach to protection (relevant for meeting new E.U. General Data Protection Regulation requirements into effect since May 25, 2018);
- » Implement system-wide data encryption and mechanisms for data protection including off-site cloud usage and communications,
- » Defend network access through mobile devices, including use of dedicated encryption keys or other mechanism for data protection (such as tokenization or data masking/obfuscation);
- » Test data redundancy measures by disconnecting data center, bringing systems down, and back into service using data backup.

Establish a risk mitigation strategy to quantify the value of the asset or risk of loss, and align security resources accordingly. Ensure compliance by users, devices and applications connected to your network.

Identify resources to execute.

Establish regular training schedule for staff on IT hygiene.

Gain best evaluation/opinion that your resources allow from informed third party on status of IT hygiene and systems to address.

Steps to take **outside** your organization...

05

Relationships with Government Partners: Identify and develop effective relationships with decision makers and stakeholders in the federal, state, and local government.

Identify government agencies' competencies and authorities (DHS, FBI trusted commercial providers):

- Geographic and jurisdictional distribution of forensic evidence;
- Advice and advocacy;
- Subpoenas, search warrants, preservation requests.

Where sensible, **participate in public-private risk partnerships** for cybersecurity and infrastructure protection risk management planning and analysis. This forward-looking, strategic engagement will complement existing incident response and information sharing efforts with government.

Communicate with law enforcement early during a crisis to leverage additional support and resources, and to clarify potential implications of investigation on crisis management processes and communication protocols, especially timing/sequencing of public disclosures.

06

Communication Priorities: Establish procedures and templates to react as quickly as possible.

Define messaging, prioritize outreach, and assign responsibility for communication with key stakeholders:

- Customers whose personal information/data has been breached;
- Relevant government law enforcement agencies charged with identifying bad actors and discretely sharing relevant information so that other companies avoid similar breaches;
- Regulators charged with oversight of the industry and its customers;
- Outside counsel;
- Organization's employees and Board of Directors;
- Business partners.

Designate a spokesperson;

Have clearly established pre-incident relationships with media outlets, and access to social media.

Business Executives for National Security | 1030 15th Street NW, Suite 200 East | Washington, D.C. 20005
Phone: (202) 296-2125 | Email: bens@bens.org | Twitter: @BENS_org