Cybersecurity for Nonprofits – What Is Noise and What Is News

October 14, 2020

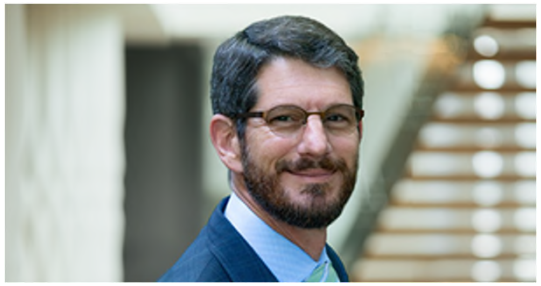
Ari M. Schwartz
Managing Director of Cybersecurity Services | +1 202.344.4711 | ASchwartz@Venable.com

Grant M. Schneider
Senior Director of Cybersecurity Services | +1 202.344.4612 | GMSchneider@Venable.com

VENABLE LLP

Who Are We?

- **Ari Schwartz**: Leading voice in national cybersecurity policy with extensive government and nonprofit sector experience.
  - White House National Security Council special assistant to the president and senior director for cybersecurity
  - Senior advisor to secretary at the Department of Commerce
  - Vice president and chief operating officer at the Center for Democracy and technology director for Federal Cybersecurity under President Barack Obama



- **Grant Schneide**r: Leader in the cybersecurity sector with extensive experience driving organizational change, developing policy, and driving enterprise-wide technology modernization.
  - Federal chief information security officer, Office of Management and Budget
  - White House National Security Council special assistant to the president and senior director for cybersecurity
  - Chief information officer, Defense Intelligence Agency

VENABLE LLP

Cybersecurity Overview

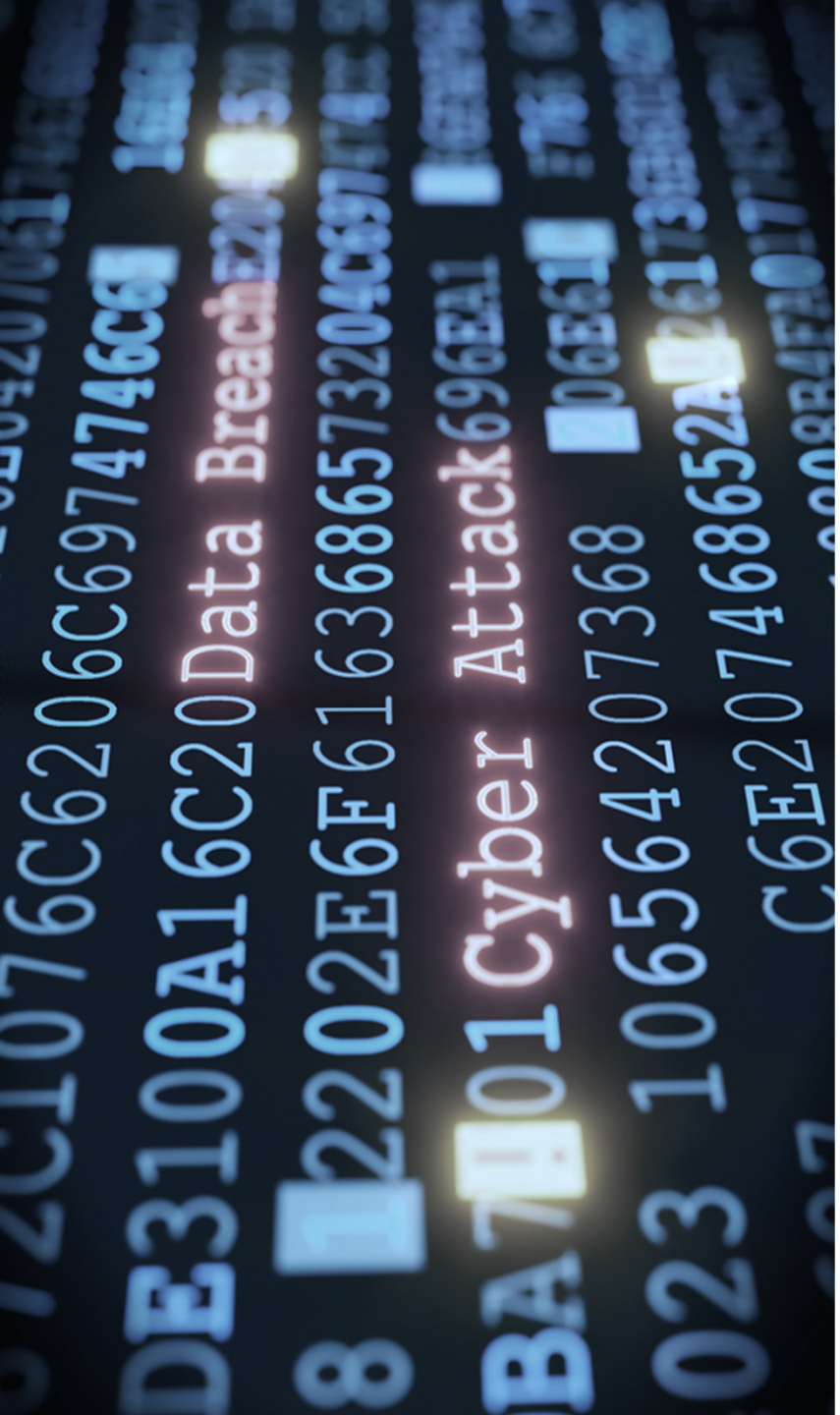
Confidentiality

Integrity

Availability

Which means:

- Preventing information from being taken without permission
- Preventing information from being altered without permission
- Preventing information or services from becoming unavailable



The Threat

Nation-States

Cybercrime

Hacktivists

Working Remotely: What are we concerned about?

Incidents are increasing

- Half of all organizations report having incidents in the first half of this year
- Most of these incidents were tied to remote work

(source: Tessian)

This trend is consistent with what Venable is seeing with its clients

Most frequent incidents that Venable sees among nonprofit clients:

- Account takeover and/or phishing leading to:
  - Billing fraud
  - HR identity theft
- Ransomware

VENABLE LLP

Understand Your Risk

People. Process. Technology.

- C-Suite buy-in from the beginning
- Any baseline is better that none, but not all are equal
- Getting started is often the hardest part
- Fully integrate cyber into enterprise risk management

VENABLE LLP

NIST Cybersecurity Framework

- Developed in consultation with industry over a one-year period
- Originally required by the Obama administration to have a more systematic way of addressing critical infrastructure risk
  - However, it has gained popularity across all public/private sectors and even internationally
- It is mapped to a wide range of U.S. and international standards

NIST Cybersecurity Framework – Key Activities

1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

VENABLE LLP

Questions?

VENABLE LLP

VENABLE LLP