ADVANCED CYBER SECURITY CENTER

Engaging With Law Enforcement: A Conversation With Pat Ford

Americas Cybersecurity VP & CISO
Schneider Electric

Cyber Risk Governance Executive Practice Guide

May 2024

TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.

ADVANCED CYBER SECURITY CENTER

Pat Ford
Americas Cybersecurity VP & CISO
Schneider Electric

Erin Joe
Cybersecurity Executive, Office of the CISO
Google

On May 1 at the ACSC Cyber Risk Governance Workshop, hosted by Google in Cambridge, we featured two private sector security executives whose distinguished careers as FBI Special Agents gave them unique insights on how to collaborate with law enforcement.

"You don't want to have to make new friends during an incident."

Who Can Help And What To Expect

Key takeaways: Deciding when, where, and how to engage with law enforcement can directly impact your ability to respond and recover when an incident occurs.

- Proactively establish ongoing relationships with regional law enforcement staff, before an incident occurs.
- Understand how local agencies and offices are staffed and organized—and how to work with them.

Before a crisis, it's critical to understand the mix of agencies and resources that may become involved with any specific incident.

- There is a mix of government agencies that all have different cyber missions, roles, responsibilities, and capabilities.
- These include the Federal Bureau of Investigation (FBI), US Secret Service (USSS), Department of Homeland Security - Cybersecurity Infrastructure Security Agency (DHS CISA), the U.S. Attorney's Office, local law enforcement, and several federal and state regulatory agencies.
- Agencies typically coordinate very well, so information reported to one federal agency will be disseminated to the other agencies.
- Some incidents may have both a criminal and national security component.

Contact Us
(617) 485-1112
wguenther@acscenter.org

ADVANCED CYBER SECURITY CENTER

“Reach out to understand who gets involved and when”

A number of factors, including the nature of the incident, determine which agency may take the lead.

- A single incident might involve elements of criminality, fraud, and even national security.
- FBI offices staff along these lines, but are used to collaborating in teams.
- CISA is increasingly becoming the lead agency for federal involvement in prevention and recovery, especially for entitles in the critical infrastructure.
- Depending on the type of threat, agencies may have specific resources assigned (e.g. ransomware groups assigned to specific field offices/agents/data scientists in the FBI).
- It is always recommended, even after contacting law enforcement directly, to report the incident via the IC3.gov website.

The specifics of the incident (and your industry) determine when you engage law enforcement.

- The decision to partner with law enforcement may involve risk mitigation, containment, recovery, intelligence gathering, and disclosure.
- Leadership should be aware of and approve how and when to engage law enforcement in an incident response plan. A good practice is to include law enforcement interaction in your playbook, crisis simulation and incident response policy.
- In most cases, speed is everything; reaching out early is optimal when it’s deemed appropriate.

Incident After-Action Briefings are valuable for management - and for boards

Clear procedures on when and how to engage board leadership will improve confidence in incident response. Incident after-action reports are an opportunity to inform boards of larger security issues.

Read more about that here.

Contact Us

(617) 485-1112

wguenther@acscenter.org

ADVANCED CYBER SECURITY CENTER

Practical Steps To Engage With Law Enforcement

"Law enforcement has specific resources – like ransomware keys – they can help."

Before an incident, collaborate formally and informally.

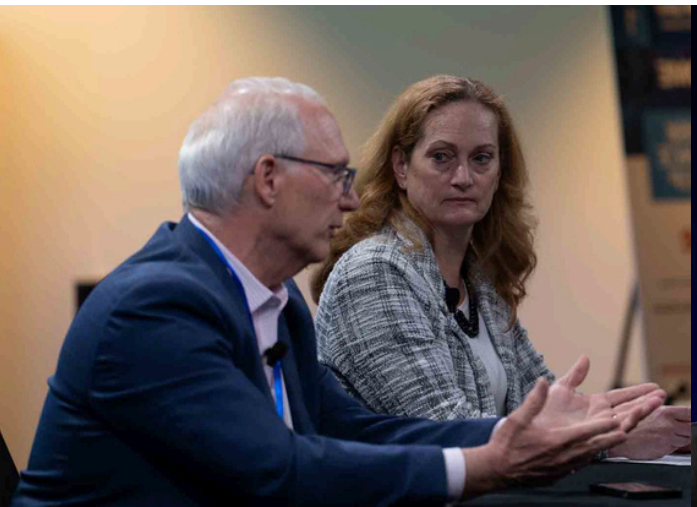
- Reach out to meet and greet local FBI office and develop personal relationships
- Formally collaborate by joining the DSAC private/public working group
- Owners and operators in the current 16 CIP sectors can join InfraGard

During an incident, leverage law enforcement's expertise and resources, and provide information you have developed.

- Reach out to meet your incident team (agents, data scientists, threat specialists)
- Brief them on the incident and response to get them up to speed
- Get feedback: How well are you doing? What are you missing?
- Provide law enforcement with any IOC's or intelligence you have identified during your response. This information can be shared to prevent others from becoming a victim or to respond effectively.
- Remain in contact with law enforcement as they may be able to offer assistance on what to expect next and help you anticipate future actions.

About the ACSC

The Boston-based ACSC advances member cyber defense strategies through regional, national and global practice-sharing networks of industry leaders and provides professional opportunities for rising talent. This Executive Practice Guide reflects key takeaways, with proprietary information redacted, from this NDA-covered session.



Contact Us

(617) 485-1112

wguenther@acscenter.org