Reasonable Security Program Evaluation & Measurement

July 13, 2020

CORVEL

CRYPSIS™

MUNGER TOLLES & OLSON LLP

1

Panel Speakers

Art Ehuan
VP
Crypsis Group



Art Ehuan, is an expert in cyber risk management and cyber investigations. He joined Crypsis after managing the Global Cyber Risk Services practice at the global professional services firm Alvarez & Marsal, where he led client engagements on strategic cyber risk and protection strategies for both U.S. and international customers. He is a former FBI supervisory special agent with last assignment in the cyber crime investigations unit at FBI HQ.

LeeAnne Pelzer
Principal Consultant
Crypsis Group



LeeAnne Pelzer is a cyber risk management specialist with consulting and advisory experience in both the commercial and federal sectors. She joined Crypsis in 2019 from Deloitte & Touche LLP, where she developed an expertise in risk scoring, risk prioritization, and proactive cyber risk management. LeeAnne has delivered professional services to some of the largest and most complex organizations and agencies in the United States.

Robyn Bacon,
Attorney
Munger, Tolles & Olson LLP



Robyn Bacon is a partner in the Los Angeles office of Munger, Tolles & Olson. A former federal prosecutor with significant experience in both the government and the private sector, Ms. Bacon focuses her practice on cybersecurity and data privacy, complex commercial litigation, trial advocacy and white collar defense and investigations.

Stefan Richards
vCISO
CorVel



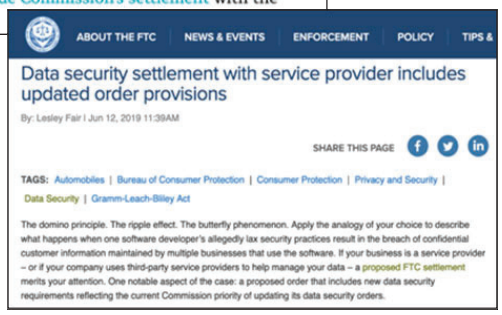
Stefan Richards serves as the Chief Information Security Officer for CorVel Corporation. Stefan was previously the CISO for the State of Oregon and Intel – GE Innovations.

2

Why is a "Reasonable Security" Evaluation Necessary?

- **Ensures organizations take due care** when implementing protective measures and security controls
- **Validates the effectiveness** of the granular components of an organization's information security program
- **Evaluates and confirms cyber risk management** activities and risk mitigation efforts
- **Protects** customers, clients, employees, and brand / organizational reputation





FTC Enforcement Action Evaluated Against NIST CSF

- "***The FTC has recognized that there is no such thing as perfect security***, *and that security is a continuing process of detecting risks and adjusting one's security program and defenses.*"
- "***The Framework and the FTC's approach are fully consistent***: *The types of things the Framework calls for organizations to evaluate are the types of things the FTC has been evaluating for years in its Section 5 enforcement to determine whether a company's data security and its processes are reasonable.*"

The FTC has brought enforcement cases against companies that didn't implement certain data security practices which also align with the following **Protect** action steps:

- Manage identities and credentials for authorized devices and users;
- Manage and protect physical access to assets;
- Manage remote access;
- Manage access permissions, incorporating the principles of least privilege and separation of duties;
- Protect network integrity, incorporating network segregation where appropriate;
- Inform and train all users;
- Ensure privileged users understand roles and responsibilities;
- Ensure third-party stakeholders understand roles and responsibilities;
- Protect data-at-rest;
- Protect data-in-transit;
- Formally manage assets throughout removal, transfers, and disposition;
- Implement protections against data leaks;
- Use integrity checking mechanisms to verify software, firmware, and information integrity;
- Destroy data according to policy;
- Develop and implement a vulnerability management plan;
- Perform maintenance & repair of organizational assets and log them in a timely manner, with approved and controlled tools;
- Protect removable media and restrict its use according to policy; and
- Control access to systems and assets, incorporating the principle of least functionality.

The FTC has brought enforcement cases against companies that didn't implement certain data security practices which also align with the following **Detect** action steps:

- Aggregate and correlate event data from multiple sources and sensors;
- Monitor the network to detect potential cybersecurity events;
- Monitor personnel activity to detect potential cybersecurity events;
- Monitor for unauthorized personnel, connections, devices, and software; and
- Communicate event detection information to appropriate parties.

The FTC has brought enforcement cases against companies that didn't implement certain data security practices which also align with the following **Identify** action steps:

- Establish an organizational information security policy;
- Coordinate and align information security roles and responsibilities with internal and external partners;
- Identify and document asset vulnerabilities;
- Receive threat and vulnerability information from information sharing forums and sources;
- Identify and document threats, both internal and external;
- Use threats, vulnerabilities, likelihoods, and impacts to determine risk;
- Establish and manage risk management processes that are agreed to by organizational stakeholders;
- Inventory physical devices and systems within the organization; and
- Establish cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders.

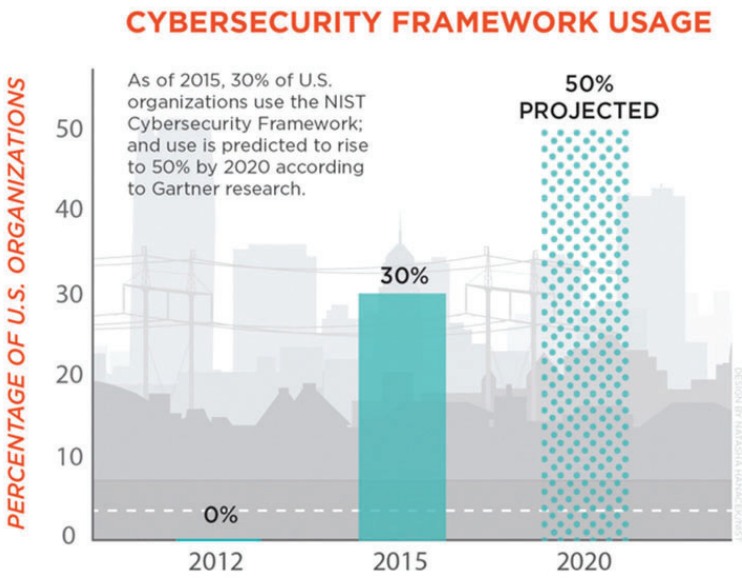
The FTC has brought enforcement cases against companies that didn't implement certain data security practices which also align with the following **Respond** action steps:

- Execute response plans during or after an event;
- Share information consistent with response plans;
- Coordinate with stakeholders consistent with response plans;
- Investigate notifications from detection systems;
- Understand the impact of an incident; and
- Contain incidents.

https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc

Evaluate Reasonable Security Against A Framework / Standard

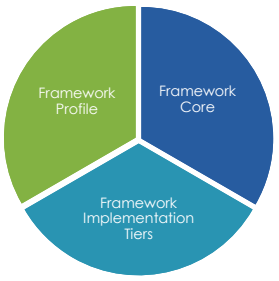
- NIST Cybersecurity Framework (NIST CSF)
- Center for Internet Security (CIS) 20
- International Standards Organization (ISO) 27001/2

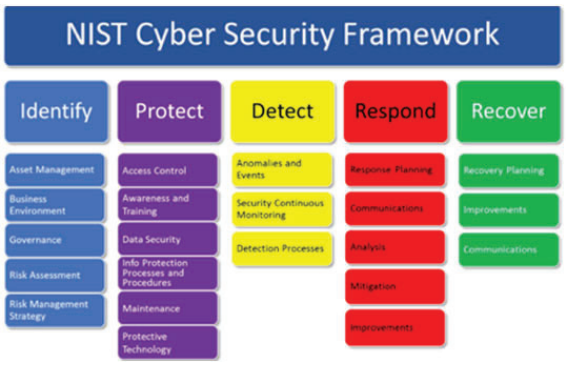


https://www.nist.gov/industry-impacts/cybersecurity-framework

NIST Cybersecurity Framework

- **Framework Core**: Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls
- **Framework Profiles**: Alignment of an organization's requirements and objectives, risk appetite, and resources using the desired outcomes of the Framework Core
- **Framework Implementation Tiers**: A qualitative measure of organizational cybersecurity risk management practices





https://www.nist.gov/industry-impacts/cybersecurity-framework

UT LAW CLE THE UNIVERSITY OF TEXAS TEXASLAW

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the UT Law CLE eLibrary (utcle.org/elibrary)

Title search: Reasonable Security Program Evaluation & Measurement

Also available as part of the eCourse
2020 Essential Cybersecurity Law eConference

First appeared as part of the conference materials for the
2020 Essential Cybersecurity Law session
"Is Reasonable Security Achievable in the Corporation?"