Compliance Simplified

The Most Interesting Talk Today!

security fanatics™

NICK ESPINOSA

- Chief Security Fanatic of Security Fanatics
- CIO of BSSi2
- Professional Hacker
- Member of the Forbes Technology Council
- Regular contributor for Forbes.com & Smerconish.com
- Co-author of an Amazon Best Selling book “Easy Prey”
- Nationally syndicated radio show host of “The Deep Dive”
- TEDx Presenter
- Board Member | College of Arts and Sciences, Roosevelt University
- Board Member | Center for Information and Cybersecurity
- Board Member | Bits N’ Bytes Cybersecurity Education
- Board Member | KEEN Chicago

US Compliance Law Is A Hot Mess!

- We have no single comprehensive federal law regulating the collection and use of personal data.
- Our patchwork of state, federal and self-regulatory compliance laws overlap and can even contradict each other.
- Many regulations continue to expand with new rules and policies added. Consider:
    - HIPAA in 1996 was 72,602 words long (gpo.gov)
    - PCI 3.2.1 is 17 individual documents updated independently between April 2015 and June 2018 (pcisecuritystandards.org)
    - SEC's "Questions Advisers Should Ask" alone is 5,912 words (sec.gov)
    - SOX's congressional bill was 29,852 words (congress.gov)
    - The IRS Tax Code's latest rules is 2,600 pages long…
    - With 71,354 pages of addendums, explanations, past statues and more! (irs.gov)

Cutting Through The Red Tape

Our Goals for Today:

- Understand the foundational concepts that compliance laws for data security are built on.
- Learn about the 3 core fundamentals that are the umbrella for all compliance governance.
- Discuss the “safeguards” methodology.
- Dive into the basics of a foundational Cybersecurity Framework that is almost universally used.
- Understand the core technology needed to properly build a compliant Cyberdefense strategy.

The C.I.A. Is Your Best Friend!

- The Federal Information Security Management Act (FISMA) of 2002 has become the basis for most data compliance standards within the USA.
- Understanding FISMA's "Triad" lets you and your client understand the goals of whatever compliance they fall into.
- The Triad, or CIA is:
  - Confidentiality – preserving authorized restrictions on access and disclosure, which includes means for protecting personal privacy and confidential data.
  - Integrity – guarding against improper data modification or destruction and ensuring data accuracy and authenticity.
  - Availability – ensuring timely and reliable access to the confidential data.
- THE GOAL HERE IS TO FOCUS ON AND PROTECT THE DATA!

Safeguards Are Unavoidable

Now that we understand the C.I.A. concept we need to look at how this applies to daily corporate structure and use.

- The Safeguards, or Controls, are designed to look at an organization holistically from three primary aspects:
    - Technical – the technology, and its policies and procedures for its use, that is in place to defend confidential data as well as to control access to it.
    - Physical – the physical measures, as well as the policies and procedures, used to protect confidential data from the unauthorized physical access and also protection from natural and environment hazards.
    - Administrative – the maintenance, policies and procedures with regard to the security measures that protect confidential data.
- It is a common misconception that these are used ONLY for HIPAA!

Knocking Out 95% Of It – Cybersecurity Framework

- Understanding the concept of data security via C.I.A. and the practical knowledge of how to safeguard it we can now build a framework!
- The most universally used Cybersecurity Framework is NIST.
- NIST, while US based, is accepted worldwide by corporations and other governments as a model for Cyberdefense.
- Other major frameworks like PCI DSS, ISO and CIS are at least partially, or fully, based on NIST's fundamentals.
- So without further ado here are the Five Functions of NIST.

NIST Function: Identify

- Identify Physical and Software assets to establish Asset Management.
- Identify The Business Environment the organization supports including its role in the supply chain and its place in the critical infrastructure sector.
- Identify Cybersecurity policies, legal and regulatory requirements to define a Governance program for Cybersecurity.
- Identify current Vulnerabilities, threats (internal and external) as well as risk response measures in order to create a Risk Assessment model.
- Identify and create a Risk Management Strategy, including Risk Tolerances.
- Identify and create a Supply Chain Risk Management strategy including priorities for defense, constraints based on position in the Supply Chain and its risks.

NIST Function: Protect

- Create Protections for Identity Management and Access Control for both physical and remote access.
- Create Awareness and Training programs including role based and privileged user training.
- Create a Data Security protection solution consistent with the Risk Strategy to protect the C.I.A. of confidential information.
- Create Processes and Procedures to maintain and manage protection of the systems and assets.
- Protect the organization through Maintenance activities, including remote assets.
- Manage the technology used to create the Cyberdefense strategy.

NIST Function: Detect

- Ensure that Anomalies and Events are detected and their potential impact is understood.
- Implement continuous Security Monitoring to discover cyberthreats and verify the effectiveness of the protective measures including network and physical activities.
- Maintain Detection Processes to have constant awareness of anomalous events.

NIST Function: Respond

- Ensure that Response Planning processes are adhered to during and after an incident.
- Manage Communication during and after the event with the organization, law enforcement and other stakeholders.
- Conduct Analysis to ensure effective response and support recovery activities, including forensics, to determine the impact of the event.
- Perform Mitigation activities to prevent expansion of an event and to resolve the incident.
- Implement Improvements to the Cyberdefense strategy based on lessons learned from the incident.

NIST Function: Recover

- Ensure that the organization implements Recovery Planning processes and procedures to restore assets and operations back to normal.
- Implement Improvements based on lessons learned and reviews of existing strategies.
- Ensure that internal and external Communications are coordinated and completed to alert all to return to normal operations.

Foundational Technology

<u>The Critical Components for Cyberdefense</u>

1) Next Generation Firewalls
2) Next Generation AntiVirus
3) Enterprise Level switches and wireless access points
4) 24/7 SIEM/SOC Monitoring for all of the above
5) Encryption systems (at rest and in transit)
6) Awareness and Training Programs

What this doesn't cover is everything beyond the technical solution such as Asset Management, Policies, Processes etc.

So Where Do We Go From Here?

<u>Considerations that must be dealt with</u>

1) The 5% of compliance that isn't covered here
2) Making the right choices in cyberdefense technology
3) Never standing still
4) Understanding where your limitations are (not everyone should be doing compliance work!)
5) Building alliances through colleagues

Thanks For Staying Awake!

Want the slides? Email secured@securityfanatics.com

Keep Up with the latest in Cybersecurity at:

- @NickAEsp *Daily Videos!
- /NickAEsp *Daily Videos!
- /in/nickespinosa *Daily Videos!
- www.securityfanatics.com
- www.soundcloud.com/infosecgurus *Past Radio Shows