Workforce Training: Challenges in Compliance and Information Security

Mark Boutwell
June 2018

Challenges

- Easing standards do not result in efficient and effective compliance.
- Threats keep pace with, or exceed, advances in compliance and security tradecraft.
- Human risks to compliance and security often overshadow the technical risks.
- Vulnerability mitigation will not result in getting out in front of the threat to ensure quick recovery and sustaining services.
- Compliance and security professionals often become a stovepipe tradecraft within the organization.

We Are Connected

- Google
  - intitle:"active webcam page"
  - intitle:snc-z20 inurl:home/
- Shodan
  - netgear port:80
  - Arlo
- True People Search
- Family Tree Now

Ukraine Power System Attack

SCADA Hijacking Techniques

Rogue Client
Remote SCADA Client Software

Phantom Mouse
Remote Amin Tools at OS-level

The attackers develop two SCADA Hijack approaches (one custom and one agnostic) and successfully used them across different types of SCADA/DMS implementations at three companies

Themes

- Train the workforce to meet compliance and security standards in their daily functions to create a hierarchal tradecraft implementation.
- Traditional compliance and security practices must evolve with active defense practices.
- Insider threats cannot be zero mitigated.
- Capability resiliency is preferred over vulnerability mitigation.
- Compliance and Security cross-pollination are key to awareness and understanding.

Takeaways

- Reality - people and organizations are either the direct target, an enabler, or both.
- Resiliency - vulnerability cannot be zero mitigated; humans and technology are fixed pieces in the threat landscape.
- Strategy - compliance, IT, and training functions must have awareness and understanding of the infrastructure, and of the threats to their collective disciplines.

Discussion & Questions

- The way-ahead:
  - IT modernization and policy must sync with compliance, security, and workforce training.
  - Protecting streaming data and data-at-rest (active file system, databases, application access and presentation to the user, etc).
- Implications to:
  - Talent
  - Strategic Planning
  - Modern and Legacy Technology Integration
- Use ingenuity and creativity to overcome today's paradigms to effect positive change.

"It is tough to be strategic when your pants are on fire." – Ron Kifer, VP Global IT, Hewlett Packard