Success Is A Balancing Act

Strategies for Winning in Security

Vaughn Hazen

https://www.linkedin.com/in/vaughnhazen
Disclaimer

The views and opinions expressed in this presentation do not represent those of the presenter’s employer, the presenter, or anyone else for that matter. This presentation is intended for entertainment purposes only. Your attendance in, or reading of this presentation implies your consent to hold the presenter harmless for any liability associated with your experience during this period or thoughts that may occur to you during this presentation. Leave now, if you value your time. All information and data included in this presentation are publically accessible and as a whole constitute research, not plagiarism. There is no intention to infringe on the copyright of any organization. By reading this or attending the session, you agree to hold the individual making this presentation, the sponsors, the host, the presenter’s employer, and anyone else that may be implicated, harmless for the use of publically available information. I’m trying to think of any other thing that might go wrong, and land me in hot water, and put something in here to get me out. I prefer to stay out of the fire though, so let’s look at where we’re going before we leap. Blah, Blah, Blah. Yada, Yada. Etc. so forth and so on…
How To Get Fired As A CISO *

1. **Being the Department of NO**

2. Spreading FUD (Fear, Uncertainty and Doubt)

3. Exceeding Budgets (Excessive Spending)

4. Failing to Discover or Report Significant Vulnerabilities / Risks

**CISO Tenure**

- Gartner – 4 years
- Ponemon Institute – 2.1 years

10 Immutable Laws of Security

1. If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.
2. If a bad guy can alter the OS on your computer, it's not your computer anymore.
3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
4. If you allow a bad guy to upload programs to your Web site, it's not your Web site any more.
5. Weak passwords trump strong security.
6. A computer is only as secure as the administrator is trustworthy.
7. Encrypted data is only as secure as the decryption key.
8. An out-of-date virus scanner is only marginally better than no virus scanner at all.
9. Absolute anonymity isn't practical in real life or on the Web.
10. Technology is not a panacea.

The Defense-in-Depth Model

Data
- Encryption, DLP

Application
- Application hardening, antivirus, advanced malware protection
- OS hardening, authentication, patch management, Firewall, HIPS

Host
- Network segments, IPSec, NIDS

Internal Network
- Firewalls, Network Access Control

Perimeter
- Guards, locks, tracking devices

Physical Security
- Security documents, user education, HR enforcement

Policies, Procedures, & Awareness

Balancing Act

CISO Success

Protect  Enable  Execute  Respect
Key Stakeholders

- Customers
- Shareholders
- Executives
- Employees
- Regulators

CISO Success

Enable

Protect

Execute

Respect
Successful CISO Attributes

- Curiosity
- Creativity
- Vision (Strategic Thinking)
- Adaptability
- Leadership
Summary

◊ CISOs lose their jobs for
  ◊ Saying NO too often
  ◊ Exceeding budgets
  ◊ Spreading FUD
  ◊ Not noticing or reporting significant vulnerabilities

◊ Technical principles haven’t changed much…
◊ PEER (Protect, Enable, Execute & Respect) must be in balance
◊ Key stakeholders include customers, shareholders, executives, employees and regulators

Contact me at https://www.linkedin.com/in/vaughnhazen