Navigating Organizational Decision Making for Information Security Professionals

November 17, 2015

Larry Carson, Associate Director Information Security Management

A Bit About my Role

Security Operations for all campuses

- Point Grey
- Okanagan
- Robson Square
- Hospitals (80+ endpoints)

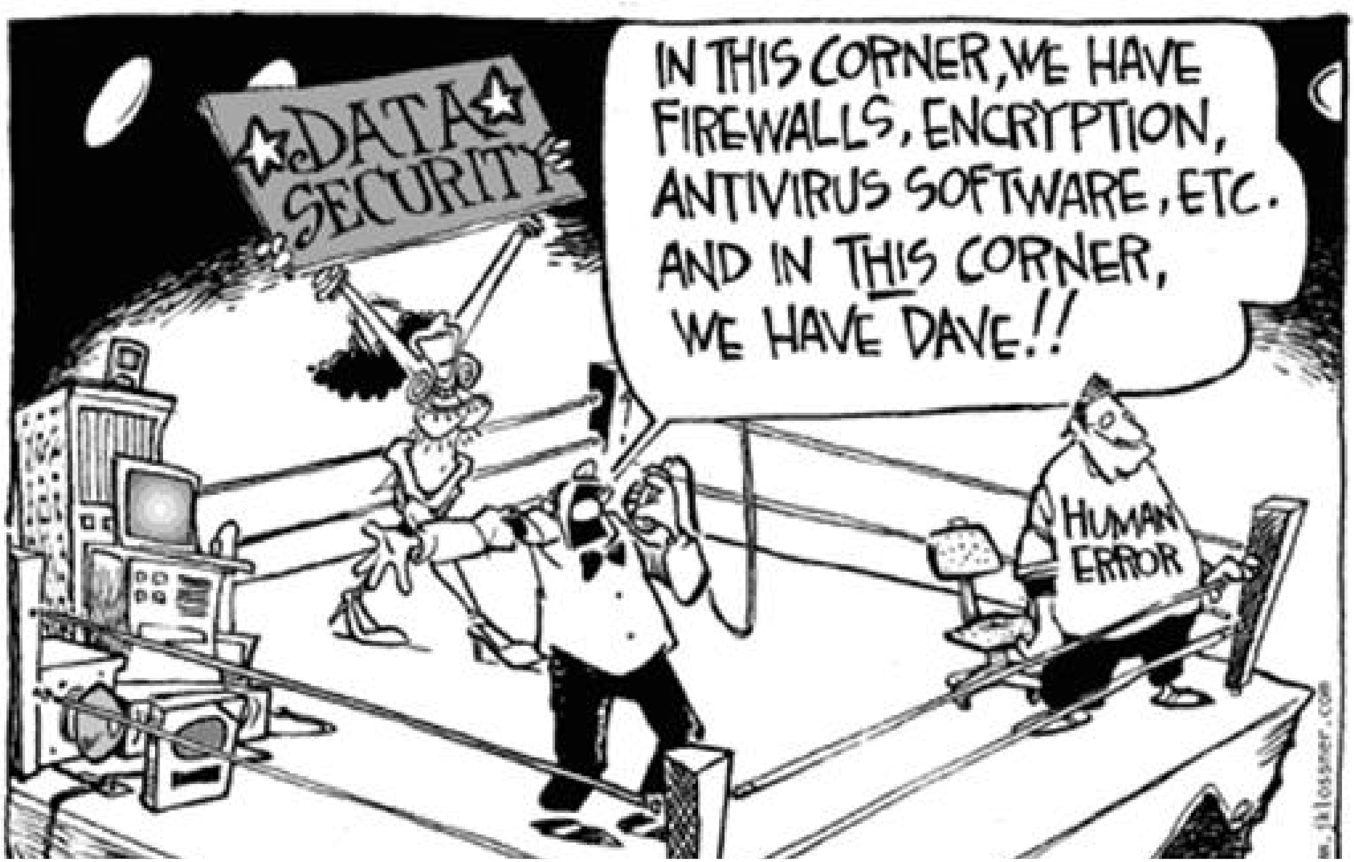
What’s that look like?

- 54,000 students
- 20,000 employees (14.5K FTEs)
- ¼ million public IPs
  - 166K Academic/Pesearch/Admin IPs
  - 14.5K Internet connected IPs

What’s the scope?

- Defense
- Incident Response
- Awareness
- STRA

What Security Really Looks Like in Organizations…


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
w.sklossner.com

Security Project Approvals and the Organization

Organizational culture and its impact

- Risk Tolerance levels
- Tone at the top
- Priorities of the org
- Approach to Project Management
- Security and privacy awareness levels

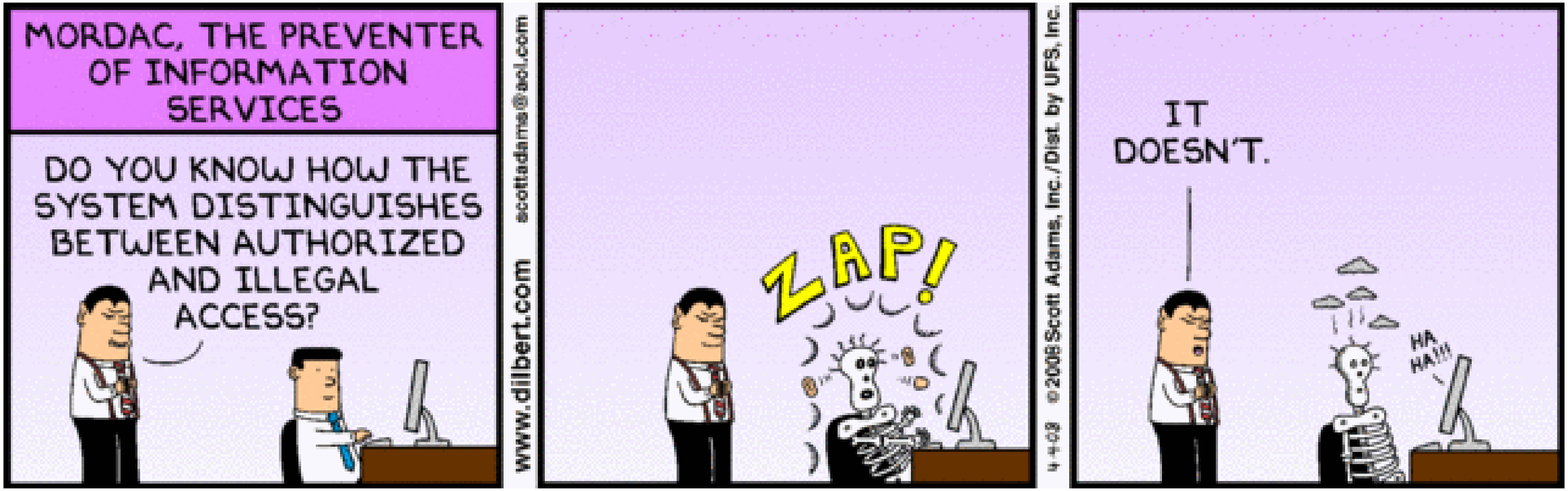
How does the project affect the bottom line

- Increase in revenue?
- Decrease in expenses?
- Lower risk?
  - Is that measurable?

Signoff

- Approval: Yes, No…
- Can approval change?
- Communicate, communicate, communicate

What People Think Security's Role is…


MORDAC, THE PREVENTER OF INFORMATION SERVICES
DO YOU KNOW HOW THE SYSTEM DISTINGUISHES BETWEEN AUTHORIZED AND ILLEGAL ACCESS?
scottadams@aol.com
www.dilbert.com
ZAP!
© 2008 Scott Adams, Inc./Dist. by UFS, Inc.
4-4-08
IT DOESN'T.
HA HA!!!

http://dilbert.com/strips/comic/2008-04-04/

IT Projects and Security's Role in the Org

When does security engage

- Project Inception/development/go-live
- How often?

What really happens

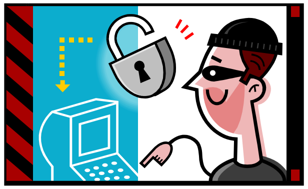
- PMO processes
- Embedding security within other teams

What are the Critical components

- Information flow
- Information at rest
- Backups
- Destruction
- Outsourcing: Cloud/hosting/SaaS/etc.

Signoff

- Approval: Yes, No…
- Next steps



Incident Response Decisions and Organizational Impact

A security incident has occurred – now what

- Shutting down a service is not as obvious as one might think. Factors:
  - Severity of compromise
  - Sensitivity of Information at Risk
  - Impact on Business (shut down vs stay up)
- Who needs to know: management/technical

Restoring services

- Workarounds
- Partial restoration/Full restoration
- Compensating controls

Managing information flow

- Messaging: internal/external
- Media: Key talking points

Technical Security Decisions: How InfoSec affects the Org

Situational awareness

- How aware is your Executive/Board of organizational security levels

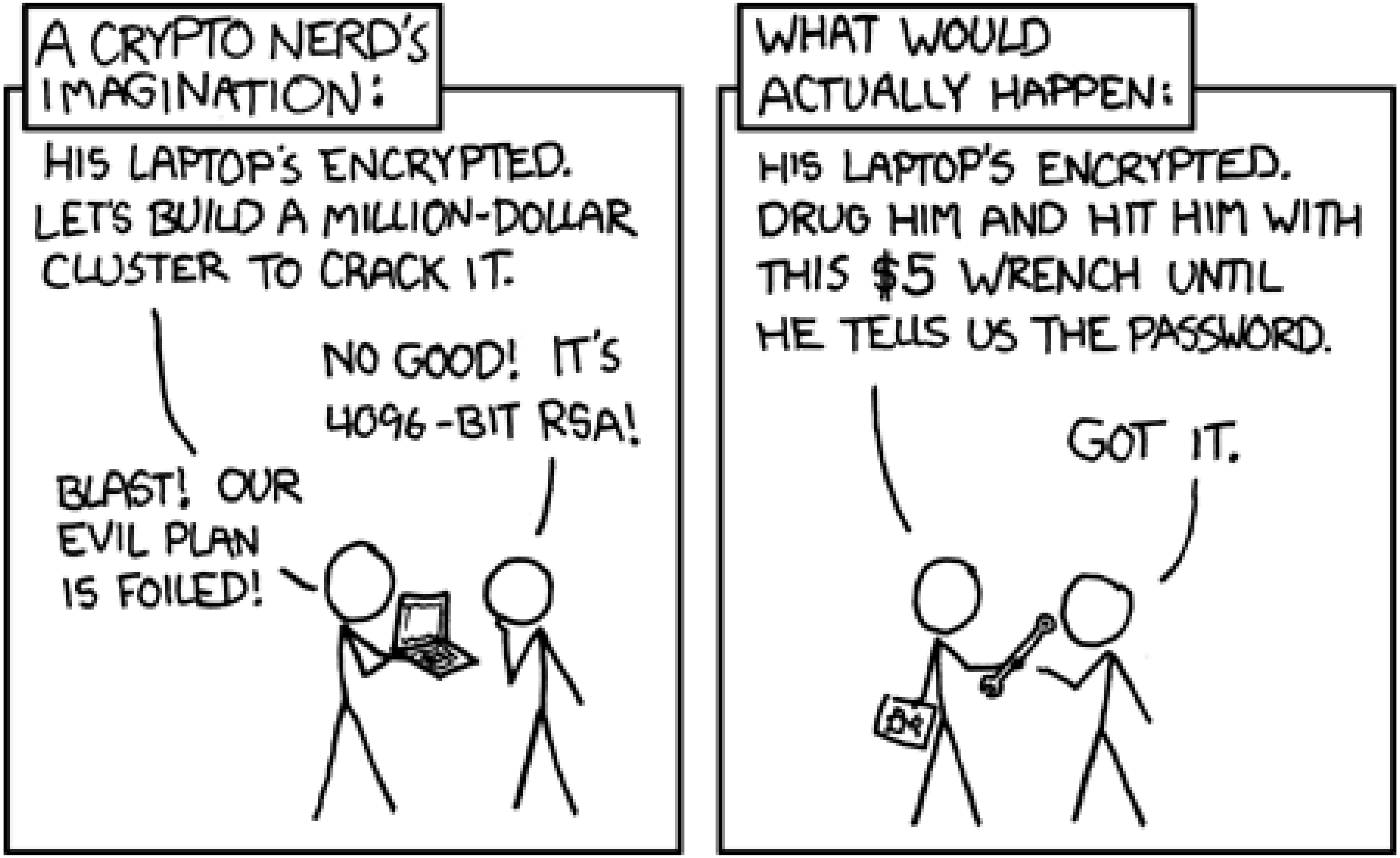
Risk Management

- Are security risks being ranked against other organizational risks
- Are risk aware decisions being made

Compliance (legal/regulatory)

- Privacy laws (FIPPA)
- Credit Card (PCI-DSS)
- Copyright Modernization Act
- CAN-SPAM
- Others

A Parting Note on Reality vs. What we Think


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LETS BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

HTTP://XKCD.COM/538/

Information Security Questions?

Contact Larry Carson,

Associate Director, Information Security Management

larry.carson@ubc.ca
604-822-0773
Twitter: @L4rryC4rson