SECURE DESIGN CONSULTING:
COMBATING THE IDEA OF ASSUMED SECURITY

Damian Romano and Jacob Penovich
“The overall impression is that the role of security in each project is based on budget, internal politics, or “business as usual,” and not executed by the principles of best practices. Simply put, this creates siloes and organizational disconnects that are complicated by insufficient communication and cooperation.”

A QUOTE ON SECURITY
PROJECT PROBLEMS

BUDGET
- Resource Expenditure
- Failed Forecast
- Scope Creep

INTERNAL POLITICS
- BU Priorities
- Executive conflict
- Sponsor influence

BUSINESS AS USUAL
- Blind spots
- Inflexibility
- Lack of understanding
THE BIG 3

1) PROJECT MANAGERS

2) DEV MANAGERS

3) POLICIES AND PROCEDURES.
THE PROJECT MANAGER

PROJECT MANAGER

PROJECT TEAM
THE DEVELOPMENT MANAGER

...Innovation
...Dev Team
...Budget

Functionality...
Deadlines...
Time-to-Market...
POLICIES AND PROCEDURES
SDLC/PROJECT BLUNDERS

Lack of visibility/knowledge of program/project initiatives.

Lack of policy/standard enforcement.

Implementation of vulnerable solutions.

Last-minute security roadblocks with bolt-on security and/or exception.
WHAT MAKES SECURITY GO BAD?
WHAT MAKES SECURITY GO BAD?

- Process (or lack thereof)
- Silo's
- Resource utilization (over/under)
- Rapid expansion
PROCESS (OR LACK THEREOF)

Common hurdles …

- New processes.
- Process in flux.
- Outdated process documents (or missing documentation)
- Poorly made processes.
SILOS AND RESOURCES

Silo's

Resource utilization (over/under)
RAPID EXPANSION!
IS SECURITY REALLY EVERYONE’S RESPONSIBILITY?
“There was an important job to be done and EVERYBODY was sure that SOMEBODY would do it. ANYBODY could have done it, but NOBODY did it. SOMEBODY got angry about that, because it was EVERYBODY’S job. EVERYBODY thought ANYBODY could do it, but NOBODY realized that EVERYBODY wouldn’t do it. It ended up that EVERYBODY blamed SOMEBODY when NOBODY did what ANYBODY could have.”
THE HUMAN FACTOR

Information Security IS Everyone’s Responsibility.

BUT...

People are often the weakest link in any security system.
WHAT'S TO BLAME?

Awareness?  
Technology outpacing?  
Skills Gap?  
Process ignorance?  
Training?

Or…
We must accept human error as inevitable – and design around that fact.

Donald Berwick
WHAT IS SECURE DESIGN CONSULTING?
COMBATING THE IDEA OF ASSUMED RESPONSIBILITY

**SDC** was established to ensure IT tools and controls are implemented and utilized in order to assure the right visibility within the grander scope of the governance of enterprise IT.
ORGANIZATIONAL POSITION

Governance, Risk, Compliance

Secure Design Consulting

Information Security

Project Management
Security Advocacy
- Assist PM and Dev team with IT security initiatives.
- Communication channel between technical and non-technical resources.

Security Context
- Standards, Policy, and Procedures.
- Exception review and consultation.

Security Validation
- To ensure solutions being brought into the Raymond James environment are secure.
- Review Test Plan, architectural changes, user entitlements, and security controls.
THREE REAL WORLD EXAMPLES

1. Robotic Process?

2. Shadow IT – SaaS?

3. Data Obfuscation?
WHY SECURE DESIGN CONSULTING? (SDC)
THE THREAT LANDSCAPE IS EVOLVING - SO WE HAVE TO EVOLVE.

Misconfigured cloud setups. (s3 exposure, databases open to the web, weak or no login to access critical resources).

Increased mobile adoption with MDM playing catchup.

IOT and all that comes with IT.
- Smart homes.
- Smart Cars
- Smart {x}
- Medical IOT.
CYBERSECURITY STATISTICS

64% of defects originate in requirement phase.

Vectors of Attack
The No. 1 way banks are attacked by cybercriminals is through their web apps, according to Verizon’s exhaustive Data Breach Investigation Report.

- Web apps: 48%
- Denial of service attacks: 34%
- Card skimmers: 7%
- Privilege misuse: 6%
- Crimeware: 3%
- Other: 2%

WHO IS AFFECTED?

- The United States ranks highest with 18.2% of all ransomware attacks.
- The financial services industry sees the highest cost from cyber crime. It costs the average business $18.3 million.
- Ransomware attacks on the healthcare industry are expected to quadruple by 2020.

Ref. Veracode, Verizon, Varonis
CYBER SAFETY NET

• Work with functional teams to ensure policy and standards are addressed early on.
• Provide oversight as the project progresses.
• Help to push business and security concerns early in the development life cycle.

• *It’s not the upfront capital that kills you, it’s the operations and maintenance on the back end.* — Gene Kim
WHAT MAKES THIS OFFERING UNIQUE?

NOT: DevOps, DevSecOps, SecDevOps…

WORKED FINE IN DEV

OPS PROBLEM NOW
WHAT MAKES THE SDC TEAM DIFFERENT

- Business Info Security Lead (BISL)
- Vendor Risk Assessment (VRA)
- Supplier Risk
- Tech Risk

WHEN YOU HAVE THAT TEAM AT WORK,
A UNIQUE SET OF SKILLS.

How to build a cyber SWAT team.

- Build a team with people from different business units.
- Diverse backgrounds in both business and tech (if you can find them).
- Don’t keep filling the same slot keep growing diverse skillsets.
- Train to build new skills or sharpen less-used ones.
- Cross-train…cross-train…cross-train…
- Degrees are great, but without experience they can be a hurdle.
- Look for people who give back.
THINGS TO CONSIDER

• MANAGEMENT BUY-IN.
  • Getting the proper authority and sponsorship.
  • Trusted Advisor – credibility.

• HIRING WITH DIVERSITY IN MIND.
  • Unicorns don’t exist.
  • Hire people with blended skill sets - passion, desire, and willingness.
  • Problem solvers.

• TEAM OF ADVOCATES
  • Cross-departmental awareness/participation.
“Department of NO” to the “Department of KNOW”

- We have Annual Information Security Training for employees…
- What about Annual Business Training for Security professionals?
- Security Professionals need to be Business Enablers.
- “You can’t secure what you don’t understand.”
Q&A