SANDY BACKIK

Why Can’t IT and The Business Get Protection Right the First Time

DEPLOY CONTROL | REDUCE RISK
ABOUT CIPHERTECHS

Information Security Focused

Privately Held Company

Headquartered in NYC with Global Support

Full Service

Fortune 50 Clients
CIPHERTECHS OFFERINGS

WE SERVE OUR CUSTOMERS IN THE FOLLOWING AREAS:

1. AUDIT SERVICES
2. PRODUCT PROCUREMENT
3. INTEGRATION SERVICES
4. TRAINING
5. SUPPORT SERVICES
Disclaimer

• I am not an attorney or paralegal, so recommendations should be changed to match your environment.

• Attendees are not permitted to record (tape record or any other method) this session.

• Attendees can take a picture of a particular slide(s), as needed.
About Sandy

- 20+ years experience in information security
- 18+ years international trainer / presenter
- Former CISO and CSO
- Areas of IT Audit and Compliance, BCP/DR, Incident Response, Physical security, Privacy, Regulatory Compliance and Audit, Policies/Procedures, Operations, User Awareness, Third-Party Management
Agenda

• What’s happening today?
• Business Goals and objectives
• What’s old still exists
• Moving forward
What’s happening Today?

• Almost weekly breaches
• Almost weekly notices of non-compliance
• More and more records are being compromised

• After Sandy’s 20 years of trying and tons of dollars in investment, why are organizations are still struggling with cybersecurity? In fact, the problem seems to be getting worse, not better.
What’s happening Today?

- Management plays the compromise odds
- Management listening to vendor – “silver bullet”
- Caving to operational and business pushback
- Failing to explain the obvious about information threats (aka phishing)
- Assuming invulnerability
- Succumbing to fatalism
What’s happening Today?

• It’s not just a technical problem
• The rules of cyberspace are different from the physical world’s
• Cybersecurity law, policy, and practice are still not yet fully developed and continue to change and not be consistent

• “A good attack is one that engineers have never thought of.”
  -Bruce Schneier
What’s happening Today?

- Security is often an afterthought. No-one builds a digital system for the purpose of being secure. They build digital systems to do something useful.
- Security mechanisms may be viewed as a nuisance to be subverted, bypassed, or disabled.
- “If one overlooks the basement windows while assessing the risks to one’s house, it does not matter how many alarms are put on the doors and upstairs windows.” –Melissa Danforth
Familiar?

Hey the project is nearly done, we should do a security audit to...

Hold on, that's not the priority. Let's get the project started first, we'll see about that later...

Too late man, we don't have the time or the budget for that.

The site's been online for 10 days, and we haven't done any security testing, I'm nervous...

LATER...

Don't worry, we'll take care of it later...

DOWN! THE SITE IS DOWN! WE'VE BEEN HACKED!

How could you let this happen!?
Business Goals and Objectives

- Strategic objectives are statements that indicate what is critical or important in your organizational strategy.
  - Create opportunities for sustainability
  - Increase the movement
  - Provide the right products to our customers
  - Provide the best support to our customers
  - Have a social impact
  - Innovation
Business Goals and Objectives

- Principles are a foundation for a system of belief or behavior or for a chain of reasoning.
  - Live with integrity
  - Curious
  - Empathy
  - Persevere
  - Safety
  - Ethics
Business Goals and Objectives

• Priority is the fact or condition of being regarded or treated as more important.
  • Investment in product technologies
  • Diversity
  • Culture
  • Product expansion
  • Fast to market
All Layers involved with protection

Source unknown
What’s old Still Exists – 2009 SANS Top Programming Issues

- Improper Input Validation
- Improper Encoding or Escaping of Output
- Failure to Preserve SQL Query Structure (aka 'SQL Injection')
- Failure to Preserve Web Page Structure (aka 'Cross-site Scripting')
- Failure to Preserve OS Command Structure (aka 'OS Command Injection')
- Cleartext Transmission of Sensitive Information
- Cross-Site Request Forgery (CSRF)
- Race Condition
- Error Message Information Leak
- Failure to Constrain Operations within the Bounds of a Memory Buffer
- External Control of Critical State Data
- External Control of File Name or Path
- Untrusted Search Path
- Failure to Control Generation of Code (aka 'Code Injection')
What’s old Still Exists – 2009 SANS Top Programming Issues

- Download of Code Without Integrity Check
- Improper Resource Shutdown or Release
- Improper Initialization
- Incorrect Calculation
- Improper Access Control (Authorization)
- Use of a Broken or Risky Cryptographic Algorithm
- Hard-Coded Password
- Insecure Permission Assignment for Critical Resource
- Use of Insufficiently Random Values
- Execution with Unnecessary Privileges
- Client-Side Enforcement of Server-Side Security
What’s old Still Exists – OWASP Top 10 from 2017

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration

- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring
Oldies but goodies

• Perfect security is probably impossible in any useful system.
• “The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it.” – Robert H. Morris, former Chief Scientist of the National Computer Security Center (early 1980’s)
• “Unfortunately the only way to really protect [your computer] right now is to turn it off, disconnect it from the Internet, encase it in cement and bury it 100 feet below the ground.” – Prof. Fred Chang, former director of research at NSA (2009)
If Security Gets In the Way

- Security is meant to prevent bad things from happening; one side-effect is often to prevent useful things from happening.
- Typically, a tradeoff is necessary between security and other important project goals: functionality, usability, efficiency, time-to-market, and simplicity.
We have to move forward to Protect

- SMART Goals are:
  - **Specific** – Is the goal specific enough for clarity?
  - **Measurable** – Is there a way to measure the goal? In other words, how do you know you achieved the goal?
  - **Attainable** – Is the goal truly attainable? Or is it such an outlandish goal that it looks good on paper but is nearly impossible to complete.
  - **Realistic** – Did you write the goal realistically? For example, did you address all the challenges of completing the goal and provide the necessary resources.
  - **Timely** – Is there a timeline associated with the goal to ensure a completion date?

- “If you can’t measure and monitor your goals, chances are that your employees will never achieve them and you won’t know the difference...” Managing for Dummies
(Apologies to Mr. Adams and my fellow architects)

There is never enough time (or money) to do it right the first time
There is always enough time and money to fix it over and over again

-Anonymous
Why we Need Architecture

Input

Architectural Process

Logical – but ...

First in first out/ Priority of the day

OR

Output

Yes, it’s a Kitchen/ Bathroom
Build a Formal and Approved Information Security Program

• Information security is a relative term.

• It is effective only when it is balanced with business requirements, cost, and risk mitigation.

• Learn how to determine security requirements that mesh effectively with your business objectives, create policies that work for your organization, and use technology to implement your policies.
Build a Formal and Approved Information Security Program – A Charter

• Information is an essential Company asset and is vitally important to the Company’s business operations and long-term viability. The Company must ensure that its information assets are protected in a manner that is cost-effective and that reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

• The Company’s Information Security Program will adopt a risk management approach to Information Security. The risk management approach requires the identification, assessment, and appropriate mitigation of vulnerabilities and threats that can adversely impact Company information assets.

• This Information Security Program Charter serves as the capstone document for the Information Security Program. Information Security policies define Information Security objectives in topical areas. Information Security standards provide more measurable guidance in each policy area. Information Security procedures describe how to implement the standards.
Build a Formal and Approved Information Security Program – A Mission

- The Information Security Program will use a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures that address security and privacy objectives in tandem with business and operational considerations.

- The Information Security Program and relevant policies, standards and guidelines must have the fundamental guidance, procedures, and commentary based upon the XXX framework.

- The Information Security Program will protect information assets by developing Information Security policies to identify, classify, and define protection and management objectives, and define acceptable use of Company information assets.

- The Information Security Program will reduce vulnerabilities by developing Information Security policies to assess, identify, prioritize, and manage vulnerabilities.
A Few Information Security Goals

• To strengthen internal control and prevent unauthorized and improper access to data, thereby ensuring the appropriate protection of information assets

• To appropriately protect the confidentiality, integrity, and availability of information assets

• To ensure that information is not revealed to unauthorized third parties during the process of transmission or as a result of unintentional actions

• To ensure that all information security accidents or suspected security flaws have appropriate reporting mechanisms so that superiors are notified and these incidents are appropriately investigated and handled
A Few Information Security Objectives

• To continually strengthen and improve the overall capabilities of the information security management system

• To increase professional skills in terms of information security management and technology

• To make our organization information security complete and reliable that we can achieve ???? certification standard

• To establish quantified information security goals annually through management and review meetings
Top 10 Measures You Cannot Do Without

- Strong passwords
- Strong firewall
- Install anti-virus / malware
- Patching
- Secure endpoints, especially laptops
- Secure mobile devices
- Backups
- Monitor diligently
- Be careful with e-mail, IM and surfing the Web
- Educate everyone
Working in Security

• We need to have each other’s backs
• Managing workplace processes
• Getting one step ahead, if possible
• Communication lines always open

• Remember: We are only human, not superhuman. We need a work-life balance, no matter what to “live long and prosper”.
I appreciate your time and attendance. Additional Questions?

THANK YOU,
Sandy Bacik
san-presentations@att.net
sbacik@ciphertechs.com