CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

The Human Side of Security Trade-Offs

Key Message: It's easy to think of security as a collection of technologies and tools – but people are the real key to any security effort.

Executive Summary

Security is fundamentally a people issue. Both attackers and defenders are humans with motivations, skills, and knowledge. By making it clear that all staff members and users are key to the security effort, and by giving them the level of knowledge they need to be security savvy, you can tilt the human factors of security in your organization's favor.

In this podcast, Greg Newby, chief scientist at the Arctic Region Supercomputing Center, talks about the human side of security and what it means for business leaders.

PART 1: RAISING AWARENESS AND MOTIVATION

Motivation Is the Key

Fundamentally, security is about people, not technology. Your defenders and adversaries (including insiders) are people, not systems. So, to maintain a good security stance:

- Understand your adversaries' motivations
- Motivate and train your defenders (yourself, employees, contractors) to be proactive about security

Motivating users to think of themselves as defenders can actually be difficult. Why? Someone's job description may not say much, if anything, about being diligent and well informed about security. So it needs to be made clear to employees that, "Security is everybody's business." This means, for example, that almost all users should:

- be aware of who's coming in after hours
- be conscious of who's following them into the building or through keyed doors
- ask themselves if phone calls could be from a social engineer
- avoid clicking on spam or malicious code in their email inboxes

Job Roles Play a Part

Of course, employees who play key roles in IT, e-commerce, etc. need to have even greater awareness of security.

So, consider a multi-pronged approach:

- For staff members who play key security roles or are deeply involved with technology, offer thorough, frequent training that is a job requirement.
- For other users, make security part of "safety in the workplace" training, provide periodic security updates, and design your systems so it is difficult for them to do harm.

Don't Be Afraid to Think Outside the Box

Back to motivation: How can you motivate key staff members to design more secure systems?

One way is to give them the freedom to think like your adversaries as they design systems. For example, not only this:

> “Here’s what we expect to happen during legitimate use.”

But also this:

> “Here’s what we think an attacker might do to break in, and here are some of the unintended consequences of the problems that could result.”

Thinking outside the box like this can be difficult. One way is to hire designers and/or testers who have skills similar to those of your potential adversaries. They must be ethical, on board with the organization’s mission, and very much a part of your team.

If this type of person does not fit with your corporate culture, there is another option: Consider outsourcing to a security firm for software testing, including penetration testing, dumpster diving, phishing, and social engineering.

Sidestepping Potential Problems

Now, a big concern: How can you avoid insider threat?

Look for variety on your team. Team members should have combinations of the following skills:

- leadership
- communication
- creative boundary-testing and boundary-spanning
- software skills

Also, have good transparency in your processes. Be able to examine the data flow through those processes at all stages.

How can a business leader reach out to the IT department to:

- find out what’s going on
- give them the tools they need to effectively do their jobs
- measure how well those jobs are being done

Perhaps the most important thing is setting a tone from the top. If the IT department is sending out security newsletters or reminders, staff members may not pay attention to these unless business leaders make it clear that securing key assets (identities, data, finances) is important for all users.

Trust the IT and information security teams, and put them in position to be successful by providing visible sponsorship, backing, and support.

PART 2: BUILDING A SECURITY-CONSCIOUS CULTURE

Tone from the Top

Some well-recognized Internet-based companies (that survived the dot-coms bubble burst in the early 2000s) have now built relatively security-aware cultures. Why? Concern for a significant drop in their market value if they were to have a high-profile security breach.

Conversely, a lack of leadership support and top-down oversight increases the risk of security issues, including insider threat.

Setting a strong tone from the top doesn’t mean everyone should be doing the security department’s job. It does mean:

- Everyone should be aware of and supportive of the importance of security in the organization
- There should be a baseline level of knowledge of good security practices throughout the organization

A Concrete Action Plan

Steps to take as a business leader:

1. Conduct a fairly high-level, top-down audit of what's going on in the organization. Who is responsible for security, and are they appropriately empowered and trained?
2. Sit down with a whiteboard and work through some what-if scenarios with key staff, both technical and non-technical. Include human error, security breaches affecting partners, stolen laptops, etc. See how well you understand what the risks are and how well you are prepared to meet those risks. Then allocate time and effort to correct any weaknesses.
3. Hire an external auditing firm or task a subgroup within your organization with doing a formal audit.

Pen Test with Caution

HOWEVER: Be wary of penetration testing (also known as red-teaming). It can be extremely useful, but if you are going to do it, make sure the team has permission FIRST from appropriate people at appropriate (high) levels within the organization. Consider points where the organization's network touches partner networks, etc.

Penetration testing can actually be an excellent approach to a security audit, especially at the boundaries of networks, where acquisitions may have introduced network weaknesses that have not yet been identified.

PART 3: TACKLING SECURE SOFTWARE DEVELOPMENT

The Software Engineer's Risk Trade-Off

Switching tracks from network and system design to software design:

How can a business leader help software engineers and their managers tackle security during development, rather than after the fact? And **why** should the business leader do this? What is the return on time spent building security in during the design phase?

Recognize that software is extremely complex, including the underlying systems and environment within which the software executes. Given this, problems and unintended consequences will always arise.

It's vital to consider risk. In general, every time a full, complete audit of software code is done, the number of bugs in the code is approximately halved. So:

- How many bugs are likely to be in a software program – and how many of those are likely to have security implications – based on the number of lines of code and past experience?
- How much does a code audit cost, based on past experience?
- Now, you know that by spending X dollars, you can reduce the number of bugs by about 50% to Y.

The next step is simply to determine the point of optimal risk. It may be 2 code audits, 10 code audits, or 50 code audits, depending on the software's criticality, size, and rollout scope, as well as the potential costs to the organization of an exploit targeting that software.

Managing Complexity to Manage Risk

Given that complexity is the biggest challenge in software development, make sure to require:

- documentation

- regression testing
- checking all of the boundaries on inputs

Lastly, make security acceptable to discuss within the organization. Share foibles, outcomes, solutions, and best practices with each other.

Resources

CERT's Secure Coding Initiative web site

Security certification resources

Department of Homeland Security Build Security In web site

Howard, Michael & Lipner, Steve. *The Secure Development Lifecycle*, Microsoft Press, 2006. This book describes Microsoft's Security Development Lifecycle (SDL) as one proven way to help reduce the number of software security defects during each phase of the development process. This process has been used effectively across a range of Microsoft products.

McConnell, Steve. "Software Quality at Top Speed," August 1996.

McGraw, Gary. *Software Security: Building Security In*, Addison-Wesley, 2006. This book describes in detail how to put software security into practice. It presents the topic from the two sides of software security – attack and defense, exploiting and designing, breaking and building – including a description of seven essential "touchpoints" for software security.