How can we get business to buy into application security?

Travis Ruff

Global Application Security Manager

- Cargill's security organization has existed for 2 ½ years.
- 125 total employees, 5 in application security.
- Governance over 24 development groups, 74 business units, 2,000+ business critical applications, 130,000 total employees, 66 countries and 1,800 locations.

Cargill™

Step 1:

Educate, Educate, Educate

- Application security is part of a defensive strategy, ensure that people understand how important it is.
  - Most people understand the concept of a firewall, but how many understand that it will not protect you from SQL injection?
- Build a comprehensive training program and ensure that it is appropriate for differing audiences.
  - All levels of business, from PMs and BAs to management and executive leadership are important but have widely varying requirements; training needs to accommodate everyone, which may mean tailoring it on a case by case basis.
- Do not forget about “the others”.
  - Contractors, 3rd parties, vendors, service providers and outsourcers. If security is important to you then ensure that it is important to them. Share policies, processes and best practices.

Step 2:

Set Realistic Expectations Early, Reinforce Often

- Any security initiative is going to cost time, money and resources. Ensure that the right people have heard and understand this before you get started.
  - Projects are measured by budget and schedule. People get angry when you affect either, especially when it is a surprise.
- Awareness campaigns keep you in the spotlight.
  - Market your message heavily in user groups, employee meetings, announcements or scheduled communications, the corporate intranet, posters, flyers, etc. Forget 7 times in 7 ways, try 70 times in 70 ways.
- Integrating security into existing processes will speed adoption.
  - Work with procurement, legal and process development teams to ensure you are built into their processes. Not only will this keep you engaged with important business decisions, but will be a continuous reminder for those driving them.

Step 3:

Stop Using Scare Tactics, Start Using Reality

- Incidents like TJ Maxx and Heartland Payment Systems cannot be used to justify projects.
  - Both companies are still in business, and with TJ Maxx there was barely a blip in their stock price. Continuing to reference this as a security sales pitch is using FUD. Of course there was a change in management…
- Real-world assessments and penetration testing results are much more impactful.
  - A successful penetration test makes it difficult to argue about whether a risk exists or not. When it is using the business' systems and data, it makes it relevant.
  - This builds credibility when you correlate between processes, i.e. static code analysis, an automated web app scanner and pen test all say SQL injection, and here is the result of exploiting the vulnerability.

Step 4:

Be a Value Provider, not the Department of No

- Secure software has tangible benefits besides security, ensure that the business knows this.
  - Increased uptime, fewer support tickets, decreased run costs and improved customer experiences are side effects that can partially offset costs.
- Demand a seat at the M&A table.
  - Understanding the security posture of potential acquisitions ensures no surprises post close. Estimating remediation costs moving forward can be an effective input into negotiation.
- Know that consistently saying “No” will result in a change of position, probably for you.
  - Business wants to publish critical data externally, they want to collect personal information and they want it now. It is time to move from “No” to, “Yes, and here is what you need to do, and here’s the risk…”

Step 5:

Stop Talking Security, Start Talking Risk

- The business needs to understand terms like threat, vulnerability, probability and impact in technology risk terms.
  - They already understand this in business risk terms (think competitors, market fluctuations, technology changes), help them make the transition.
- Work with your business partners to understand how risk tolerant or averse they are.
  - Go in knowing that their risk tolerance may be significantly different than your own. This can and will cause you a great deal of stress.
- Ensure that everyone sees the entire universe of risk.
  - Just as application security expects the business to understand technology risk, the business expects application security to understand business risk.

Step 6:

Give the Business a Voice

- Not all vulnerabilities necessarily need to be remediated (or at least remediated immediately) so ensure you are using your limited resources in the right places.
  - Build a tiered governance model that sets clear boundaries for what risks can be accepted and at what level.
- Bring business representation to policy discussions, project and process roadmaps, communication plans, etc.
  - With a representation comes ownership, and with ownership comes a desire to succeed.