APP DEVELOPMENT REVOLUTION:

ELSEVIER TAKES A NEW APPROACH TO SECURING SOFTWARE DEVELOPMENT

Contributors: Alexander J. Fry and Meron Samuel

"Security awareness works but is not typically part of formal app development curriculums. Security concerns take a back seat to form and functionality. So making developers security aware requires a revolution in app development."

Alexander J. Fry, Vice President Software Security Assurance

Transforming from a print to a digital information provider, RELX Group sought to establish themselves as a leader in web-based, digital solutions. As part of this transformation, Elsevier was becoming more agile, leveraging new distribution channels such as mobile and moving out of traditional data centers into cloud.

When parent company, RELX Group, shifted the security responsibilities to their divisions, Elsevier knew they needed to increase security maturity within application development to protect these new digital platforms from the outset. Security needed to match the agility and risk of the new platforms. A check-the-box compliance approach to security wouldn't make the cut in this new environment as the attack surface had significantly expanded.

THE DRIVING FORCE FOR CHANGE

Initially, each Elsevier development team had different levels of security maturity and lacked the resources to enforce even the baseline application security requirements. The old process was voluntary and required the development team to reach out to the security team to ask for recommendations. In the new digital ecosystem, this approach would cost too much time, leaving the new applications exposed.

The Information Security and Data Protection division (ISDP) began intensive research into security awareness solutions. In 2011, the small team determined that they did not have the personnel or expertise to roll out comprehensive, revolutionary training for Elsevier's developers on their own. Free training materials, e.g., OWASP, seemed insufficient as a standalone solution. They decided they needed a partner, a company who would remain involved throughout the transformation.

ABOUT ELSEVIER

Elsevier is a world-leading provider of information solutions that enhance the performance of science, health, and technology professionals, empowering them to make better decisions and deliver better care.

Elsevier is part of RELX Group plc, a world-leading provider of information solutions for professional customers across industries.

Company: RELX Group
Rank: #554 in the Global 2000
Industry: Printing & Publishing
Founded: 1993
Employees: 30,400
Revenue: $5.97 billion (2015)
Headquarters: London, UK

www.relx.com

THE CATALYST FOR CHANGE

In partnering with Security Innovation, the ISDP established a formal training program for software developers with the following goals: increase security awareness, elevate and standardize security understanding, and keep pace with the digital transformation. While the initial training focused on awareness, the CISO and his team wanted a curriculum that increased in difficulty with tiers for different security stakeholders in the development teams and could cover the various platforms and technologies they were developing for/with. Demonstrable security awareness needed to become a key performance objective of every developer.

Elsevier's Software Security Assurance team developed a secure SDLC model for Agile. The model illustrates the integration of security testing throughout the SDLC and complements the courses. The courses help justify adherence to and reinforce this model.

WHY SECURITY INNOVATION?

Elsevier wanted to improve the security and thereby the quality of applications and information technology platforms in order to better meet the company's mission to empower science, health, and technology through cutting edge information solutions. The new Elsevier Information Security and Data Protection (ISDP) division began the process to improve and ensure application and information security.

Elsevier's CISO met Security Innovation's CEO at a conference in October 2011, shortly after the ISDP was formed and while they were still developing the Application Security Center of Excellence (COE). Elsevier's VP of Software Security Assurance and the CISO carefully reviewed Security Innovation's courses. The quality and depth of the courses impressed them – in particular, the ability to deliver comprehensive training for each team role. Security Innovation's willingness to engage in a conversation and adapt to feedback equally impressed them. After reviewing more than ten training providers, the information security team found a partner to co-create a repeatable, standard, and measurable security ecosystem within the development teams.

THE TRANSFORMATION

1. Security Innovation started slowly by rolling out just one course, the fundamentals of application security. The feedback received helped guide the team in structuring subsequent curriculums that increase in depth and difficulty.

2. The employees who showed a strong interest in the security training were identified as possible candidates for the Software Security Champions initiative.

3. After engaging developers, they became empowered to lead and share security best practices within their organizations. When you have a small group of security experts, it is vitally important that you cultivate a "Train the Trainers" approach, allowing security leaders to emerge from within the organization.

INNOVATION & VALUE DELIVERED

- Less time spent patch fixing retroactive security discoveries
- Overall security awareness at the software development level
- Increasingly effective and security minded development team
- Empowered developers prevent security issues before they arise
- Standardized security levels
- Security viewed in terms of quality

THE IMPACT

Prior to creating the security awareness-training program, Elsevier had a compliance-driven approach to security matters. This check-the-box approach to mainly voluntary compliance frameworks left gaping holes in security. They also had insufficient controls in place to enforce security. Without a new approach, the increasing deployment of applications would mean an increasingly resource-intensive patch-fix approach to security. With Security Innovation as a key partner, Elsevier took a proactive approach to make security a key differentiator for its business.

Initially, Elsevier selected a small number of courses for a computer-based training program but decided eventually they wanted to roll out a greater number of courses, prompting them to seek buy-in from other divisions within RELX. Technical leads of other divisions showed interest when Elsevier demonstrated success in driving forward a more successful and secure software development lifecycle. This enabled Software Security Assurance to increase the depth and difficulty of training. Eventually, security training (obtaining a white belt) for software development became a formal key performance objective.

THE REVOLUTION CONTINUES...

As a next phase to their security training initiative, Elsevier worked closely with Security Innovation to roll out a belt training program, a fun way to implement ongoing training that keeps developers engaged and motivated to learn more. Developers start with fundamentals in the "white belt" courses and proceed to the next level courses, dependent on their role and the technologies they are developing in.

As courses become part of key performance objectives, they are applied more broadly across divisions. In addition, each team is assigned a Software Security Champion (SSC) who is responsible for leading that team's security and is the point of contact between development and ISDP. All SSCs are required to obtain at least a green belt status. SSCs are also responsible for coming forward to articulate a need for security around a certain app being developed.

Since implementing the Belt Program, Elsevier management can measure expectations for each developer and incorporate security awareness into considerations for promotions or pay increases.

"The Belt Program is a natural progression of our partnership with Security Innovation. It allows us to create greater engagement with our developers while also driving accountability. We believe the Belt Program will increase the already substantial impact we have realized by implementing an Application Security training program."

Meron Samuel, Program Manager
Information Security & Data Protection Office