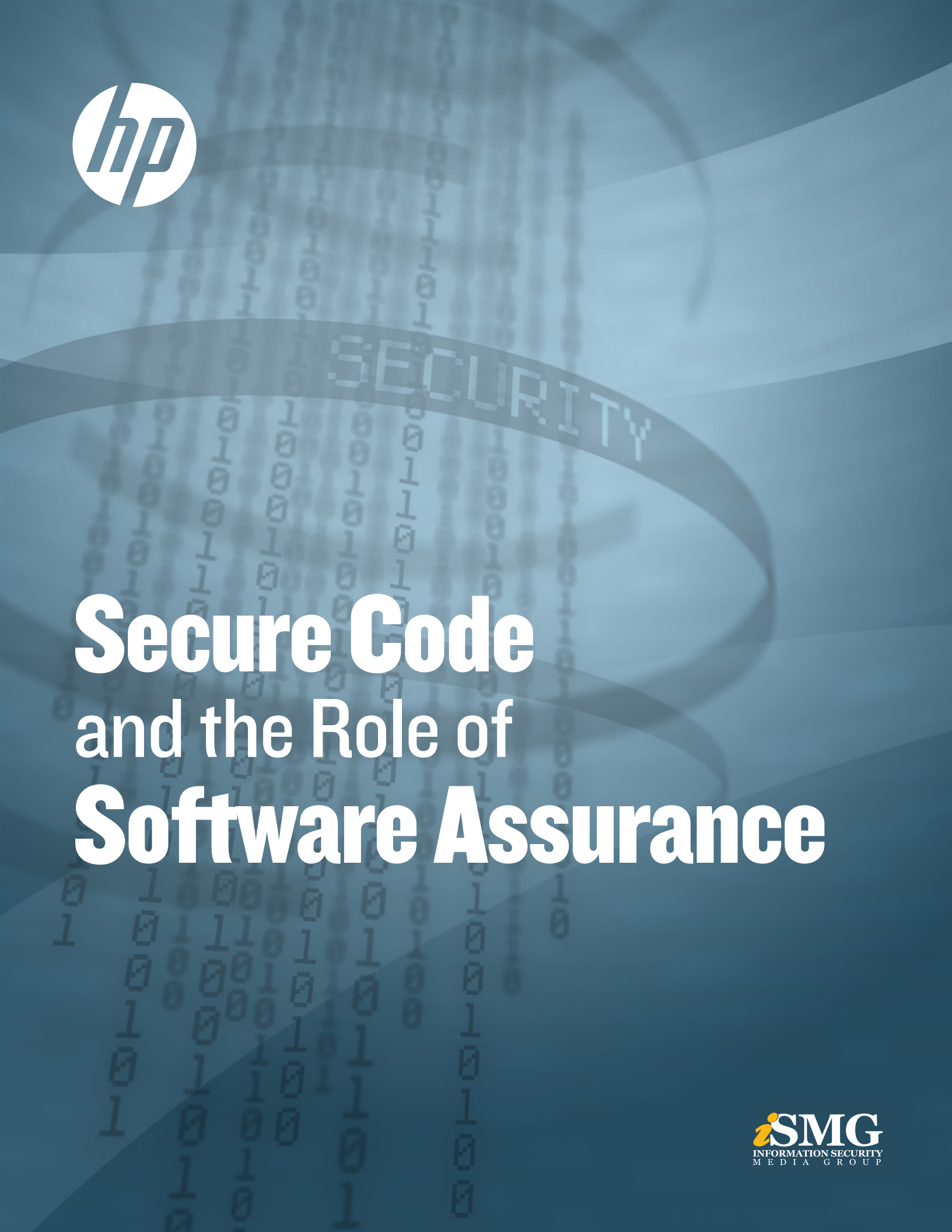


Secure Code and the Role of Software Assurance

iSMG
INFORMATION SECURITY
MEDIA GROUP

SECURE CODE AND THE ROLE OF SOFTWARE ASSURANCE

Hackers prey on weaknesses. Unfortunately, too often, companies employ software with vulnerabilities that make it relatively easy for third parties to breach the company's defenses.

With a spate of recent breaches taking place at well-known companies including Target, Home Depot and Sony, organizations must reevaluate the security of the code running within the enterprise. Leaving flawed code in place almost invites hackers in to the company's network.

Why has application security not kept pace with changes in the threat landscape? Why do companies struggle to create secure code?

According to William Hugh Murray, a management consultant and Certified Information Security Professional with more than 40 years of experience in security, it is actually much harder than it appears to create secure code. "Programming is an inherently complex and error-prone process, made worse by our choice of languages and tools," Murray says. "Companies often include gratuitous features and functions that increase the attack surface." Murray also believes that companies sometimes tolerate the creation and deployment of poor-quality code.

The acceptance of substandard work coupled with the lack of discipline, accountability and experienced managers and developers from Murray's perspective explains why companies struggle to develop secure software and applications.

One industry expert reached for this piece has a different perspective. "In the beginning, we created software, and humans made mistakes that resulted in bugs in the code and misconfigurations," the source says. "As an industry, the market adapted and sold a 'more secure piece of software' to be placed inline, aka: firewall. This allowed the application developer of the software to focus on the primary objective – functionality – and made the job of security someone else's job and expense."

Organizations sometimes are their own worst enemy, as they focus much of their efforts in ensuring speed-to-market, while making security a secondary consideration at best.

Regardless of the catalysts for the current state of software security, with each new software deployment that contains insecure code, organizations increase the chances that a breach will take place.

In fact, for some organizations that have access to the information that hackers want, such as their customers' Personally Identifiable Information (PII), for example, the threat of a breach presents a

Why has application security not kept pace with changes in the threat landscape? Why do companies struggle to create secure code?

significant, if not immediately quantifiable, threat to the organization.

Do Executives See the Value of Secure Code?

Unfortunately, some executives are only now beginning to see the value of secure code. Many believe that the risks facing the company do not merit the investment of resources to ensure the security of the enterprise's code. The problem is viewed from an IT infrastructure perspective rather than a software perspective.

Bruce Jenkins, an application security program strategist with HP Enterprise Security, believes that executives frequently rely on an incomplete understanding of the IT environment. "Often times there is the belief that a company's marketing system – which is hosted offsite, for example – is in no way connected to the company's main IT system. 'If there is a breach of any sort, there is no way we can suffer any harm.' These assumptions are often false."

In fact, the truth is far more damaging. "Many of the marketing systems companies use collect much more data than executives believe," Jenkins says. "The data might be more sensitive than it might appear, and often times there is some sort of a connection between the marketing system and the company's main IT system, even if it is just a back office exchange of data."

Consequently, the risks that organizations take are probably greater than would be warranted if the organization conducted a robust risk analysis, believes Jenkins. He also adds that, "We tend to rationalize away the really bad stuff that could potentially happen to us. Part of that is our nature, part is organizational culture."

While an executive's view of risk may be

> "We tend to rationalize away the really bad stuff that could potentially happen to us."
>
> – Bruce Jenkins, HP

based on flawed assumptions and incomplete understanding of the risk landscape, in order to support the investment needed to ensure that an organization utilizes secure software, they must see a sustainable, structured approach that supports the creation of secure code, without affecting the company's competitive footing.

How do Breaches Typically Happen?

While news of data breaches used to be buried in the business section, today that is no longer the case. Given the size, frequency and lasting impact of breaches, news of the latest breach now lands on a newspaper's front page.

Joe Sechman, director of software security research with HP Enterprise Security, notes that today's breaches typically include four distinct phases. "Hackers must overcome an organization's perimeter defenses, migrate from system to system without raising red flags, grab the data they seek, again undetected, and transfer that data out of the organization. If the company uncovers the hackers during any of these phases, they can stop the data from leaving and prevent the breach from resulting in long-lasting damage."

The "Heartbleed" bug provides just one example of the damage that flawed code can create. In the aftermath of its discovery, web operators moved quickly to bridge the gap that allowed hackers to request data from an organization's server, such as a user's login credentials. However, hackers moved faster and while we may never know the full extent of the damage caused by the Heartbleed vulnerability, organizations can no longer ignore the threat.

If organizations need a financial incentive to ensure the deployment of secure code, they need only look to the Ponemon Institute's 2014 Cost of Cyber Crime Study that noted:

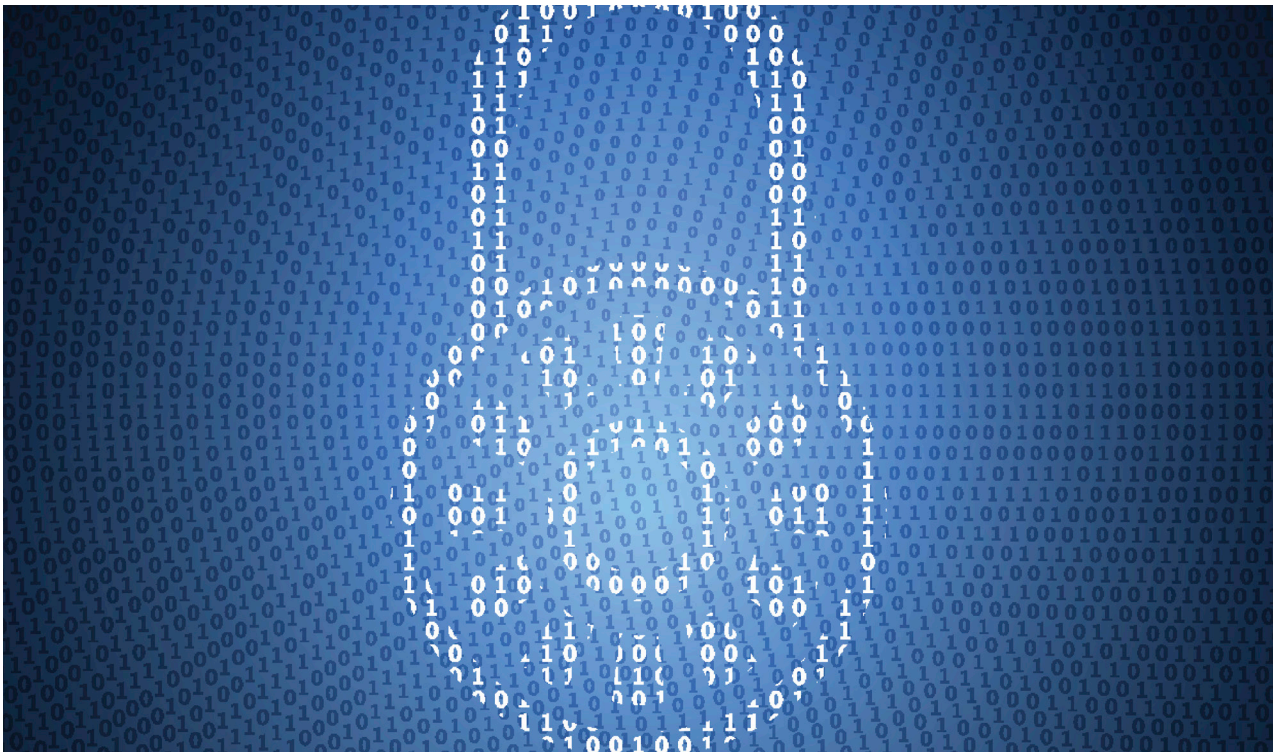
- The average cost of cyber crime: $12.7 million in the U.S., an increase of 9% over 2013 costs;
- Organizations average 138 successful cyber attacks per week, a 176% increase in five years
- The average time to resolve a cyber attack once detected was 45 days with an average cost of $1.5M; a 33% increase from 2013

How Companies Acquire, Create and Adopt Code

According to a 2014 Enterprise Software and Security Strategies survey conducted by Gatepoint Research, organizations procure, build and integrate software applications using five primary methods:

- The use of large commercial applications and the development of custom components;
- Custom in-house development;
- Application development by third parties;
- The use of open-source; and
- The development of applications externally.

While these methods involve varying levels of



control and involvement by the organization, when employed exclusively or in combination, they may result in unwittingly adopting flawed code.

In particular, when organizations outsource the development of applications to third parties, they insert greater risk. Ironically, many measure their third parties' performance based on their ability to meet deadlines. In turn, a developer may face the temptation to cut corners by recycling code, which creates common flaws for cybercriminals to exploit.

William Murray's experience tells him that there is a general failure to believe that it is cheaper to do it right the first time. "Programmers believe method, process and discipline slow them down. While they may give lip service to quality, they really believe that they are measured on speed," believes Murray.

The Benefits of Creating Secure Code

While understanding that insecure code creates risk, what are the benefits that organizations earn by improving the security of their applications? The primary benefit is that secure software prevents exploitation of an application by third parties. A 2013 study produced by Mainstay, in partnership with HP Fortify, uncovered a number of cost and productivity savings that result when companies adopt a Software Security Assurance solution, including the following:

Cost Savings:

- Reduction in FTEs Assigned to Remediation: Once implemented, SSA triggered a reduction in staff allocated with the remediation process. Instead of employing 4 to 5 FTEs to handle remediation, post-SSA implementation, organizations reduced their staff to practically zero;

On average, implementing an SSA solution and adopting related best practices reduced remediation time from 1 to 2 weeks, to 1 to 2 hours.

- Reduction in Manual Forensics: SSA reduced the need for manual forensics, which translated into an average saving of $100K per year; and
- Reduction in Compliance-Related Fees: Organizations typically experienced an 89% drop in fees paid to compliance auditors.

Productivity Savings:

- Time to Remediate: On average, implementing an SSA solution and adopting related best practices reduced remediation time from 1 to 2 weeks, to 1 to 2 hours;
- Vulnerabilities Eradicated: The percentage of repeat vulnerabilities found in software dropped from 80% to zero;
- Reduction in Development Time: Post-implementation of SSA, developers spent less time remediating coding flaws. As a result, development time per application fell by 10% to 40%. Often, developers used that time to improve existing code and complete additional projects; and
- Fewer Security-Related Product Delays: Companies experienced a reduction in the discovery of security flaws prior to product launch, which could result in delays of 3 to 4 months.

All told, organizations included in the study conservatively estimated the cost savings associated with SSA at $3M per year and productivity savings at $5M per year. In addition, the study estimated that companies could generate an additional $8.3M in revenue.

The Seven Steps to Secure Code

The 2014 Gatepoint Research survey on Enterprise Software and Security Strategies highlights a number of security-related challenges facing organizations today, including executive concerns about security within their applications, the difficulty managing the risk associated with the adoption of externally developed software, and the challenges in securing stakeholder buy-in in order to achieve software security goals.

Given the inherent complexity of improving an organization's software security coupled with the difficulties associated in driving change within the enterprise, tackling the risk associated with software security requires a structured approach with clear goals and expectations.

Improving an organization's software security and taking steps to embed security within the software development lifecycle will not occur overnight. HP Enterprise Security developed seven logical steps that organizations can readily embrace and follow. These steps, as detailed in the HP Enterprise Security Business Whitepaper, "*Seven Practical Steps to Delivering More Secure Software,*" help companies begin that journey.

STEP 1:

Quickly evaluate the current state of software security and create a plan for dealing with it throughout the development lifecycle.

STEP 2:

Specify the risks and threats to the software so they can be eliminated or mitigated before they are introduced.

STEP 3:

Review the code for security vulnerabilities introduced during development.

STEP 4:

Test and verify the code for vulnerabilities.

STEP 5:

Build a gate to prevent applications with vulnerabilities from going into production.

STEP 6:

Measure the success of the security plan so that the process can be continually improved.

STEP 7:

Educate stakeholders about security so they can implement the security plan.

Selecting a Software Security Solution

Organizations that employ flawed code within their applications provide hackers with a seemingly never-ending supply of targets. To help uncover vulnerabilities within their software code, organizations often seek out comprehensive Software Security Assurance solutions.

Such a solution not only helps uncover coding weaknesses, it also provides organizations with a program of activity to fix defects and reimagine their approach to software security, with the end goal being to produce software with the secure code needed to thwart attacks.

By adopting SSA, organizations create a number of benefits, including the ability to find and fix problems quicker as well as deploy their software faster, which in turn allows for the generation of additional revenue. They also avoid the remediation costs associated with a breach and minimize their ongoing compliance expense.

A high-performing SSA solution should include functionality and capabilities that help remediate flawed code, including: guidance on how to correct vulnerabilities uncovered, allow for cross-divisional collaboration, integrate with the organization's existing software development infrastructure, and deliver static and dynamic code testing and analysis. This type of functionality, when provided with governance capabilities that define and enforce security policies and the latest threat intelligence, lessens the burden on the IT department, and helps secure the organization in a timely and efficient manner.

HP's Bruce Jenkins believes that while securing buy-in to invest in SSA presents challenges, certain parts of organizations play a larger role than others do. "Even if you have no other buy-in, as long as you have buy-in from whoever owns the development of apps and software, you can probably make some progress."

Yet, Jenkins also stresses the importance of consensus. "To have other stakeholders onboard, there must be a common vision. The argument for getting everyone onboard is that all activities must connect to the organization's mission and goals. A common goal in the financial sector is to protect customer data. Adding mitigating strategies to the software development activities allows the organization to protect data. There is now an obvious association between resource effort and the organization's goals. From a security program support and stakeholder alignment perspective, who is going to argue that the company should not protect their customers' data?"

Justifying the creation of a Software Security Assurance program and the investment in related technology includes the following steps:

- **Create a Business Case:** The Department of Homeland Security provides organizations with several free resources to help quantify the costs and benefits to justify the investment.
- **Determine the Staffing Model to Support the SSA Program**: Some organizations hire staff to build and support the program in-house while other organizations choose to engage a managed application security testing service – others still will employ a combination of the two.
- **Identify Performance Metrics:** Justifying the investment does not end with the creation and approval of the business case. In order to increase awareness of the SSA program and the support needed to ensure its ongoing success, identify the operational metrics to share with senior executives.

The ROI of SSA: It Varies by Industry

Despite the existence of models to help organizations identify and document the return on investment associated with secure software, HP's Jenkins sees differences between industry sectors and their ability to justify the initial investment in secure software assurance.

"The financial industry is very good about conducting ROI studies to balance risk and reward. They can do that very quickly," notes Jenkins, "as opposed to the retail industry, which is very focused on marketing. They have a hard time developing risk analysis and identifying the benefits. Their focus is often on developing a go-to-marketing strategy so they can sell something."

A different set of challenges faces the energy sector. "Energy companies have focused intensely on infrastructure itself and not on software systems that make all that work. Sound software development methodologies are relatively new. So, their struggle is less about marketing, messaging and risk-reward."

While the ability to capture and report benefits varies by industry, ultimately, investing the time and effort to identify and classify the value created from implementing secure applications can help justify and sustain the effort.

Conclusion

Software vulnerabilities exist and finding them before hackers should be a top priority for all organizations. While the processes and technology to drive the creation of secure code are relatively immature, robust SSA solutions exist. Security and business leaders can no longer claim ignorance, or avoid implementing measures to ensure the creation of secure code.

About Fortify

HP Fortify's Software Security Assurance products and services protect organizations from the threats posed by security flaws in business- and mission-critical software applications. The Software Security Assurance suite, HP Fortify Software Security Center, drives down costs and security risks by automating key processes of developing and deploying secure applications. HP Fortify on Demand's managed application security testing available in the cloud provides all the tools you need to make your applications secure.

Visit HP Fortify to learn more.
http://www8.hp.com/us/en/software-solutions/application-security/

About HP Enterprise Security

With industry-leading products from ArcSight, Fortify and TippingPoint, HP delivers a comprehensive security portfolio that enables businesses to take a proactive approach to security that integrates information correlation, deep application analysis and network-level defense mechanisms. With HP Enterprise Security Products, businesses are better able to disrupt the adversary, manage risk and extend their security capabilities to better protect their organizations.

Visit HP Enterprise Security Products for more information.
http://www8.hp.com/us/en/software-solutions/enterprise-security.html

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401
info@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification.

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com