FORTIFIED SOFTWARE SECURITY

Jerry Sanchez

softserve

Over $57 million dollars have been invested in security services so far in 2018. The demand for cybersecurity professionals is at an all-time high—the profession has an unemployment rate of zero. And it's predicted that by 2020, 100% of large enterprises will require annual cybersecurity and technology risk reporting to a board of directors.

It's safe to say that security is a big deal—and growing more important every day.

If optimizing your business is about refinement and futureproofing, then doing the same for your security means taking ownership of software, presently and proactively. This pertains to legacy apps and systems requiring modernization, as well as ongoing development that ensures security management while delivering optimal experiences and actionable insights.

As a start, enterprise security fundamentals should be in place. These include: firewalls, IDS/IPS appliances, wireless security, and web/email application filtering. If these (and other fundamental security measures) are not already in place, it is premature to focus on optimization.

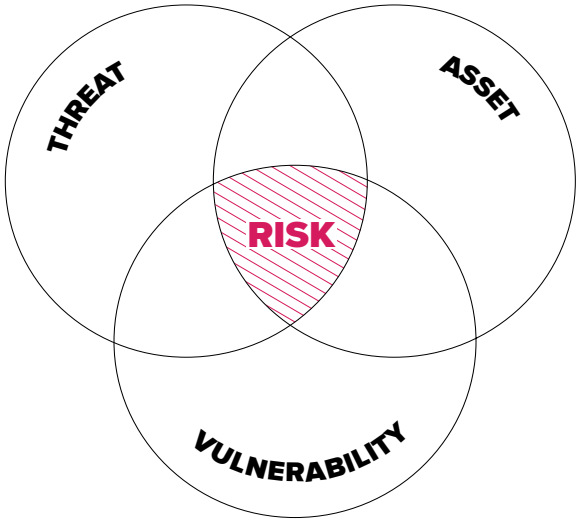
However, speaking with our clients, there are three areas of security that are consistently most pressing for those with even the most sophisticated security posture:

1. Cloud security

2. Application security assessments

3. Compliance integrity preparation

In this white paper, we'll focus on these three areas while sharing insights on event detection and vulnerability management. Most pressing for those with even the most



The security status quo isn't enough

Cause and effect: 99% of all cyber exploitation traffic is comprised of known vulnerabilities (preventable), which opens the door to 90% of all cyberattack claims stemming from human error or behavior (inevitable), as evidenced by 91% of all successful attacks beginning with a phishing email (typical).

Regular scans—focused only on critical systems—and reactive patch application is no longer a viable, standalone, vulnerability management strategy.

Security management is a layered challenge that requires a multifaceted approach, but the journey towards maturity and preparedness begins in part with:

- Acknowledging current conditions
- Resolving known issues
- Paying attention to people and processes (as well as technology)

Acknowledging current conditions
This is simply investing the time and resources in discovery to determine the "good, bad, and ugly" of current strategy and readiness—and then taking ownership of whatever is needed to formulate and act on a security strategy that's right for you. There is no room for excuses, procrastination, or de-prioritization. Breaches tend to cost far more (financially, socially, and to your brand overall) than a systematic vulnerability management plan.

Resolving known issues
If the majority of cyberattacks occur with known issues, then logic dictates that a company endeavors to resolve these issues as quickly as possible. Why knowingly remain at risk if resolution is an option? As long as there are predatory cyber criminals, there will always be new and improved issues—but for the sake of your company, remove the threat(s) before there are casualties.

People and processes
Technology has come a long way, and will go a long way towards defending against attack, but human error will continue to be a "hole" in the armor as long as people remain imperfect. You wouldn't hand the keys of an exotic sports car to an adolescent with no license, would you? Why would you make a significant investment in security and not ensure that everyone within the company is properly trained, prepared, and on guard in support of your technological counter measures?

IBM (one of our clients) provides a valuable reminder that resolving vulnerability also depends on the IT asset and its role. There is no secret formula or checklist for everyone. Patching, disabling, uninstalling, changing configuration, and upgrading are each effective

remediation options within a management program. However, the effectiveness of each of these approaches depends entirely on context.

Now let's dive into some of the biggest, current security concerns on the market.

Cloud security is no fluff

Much has been written on cloud security, and for good reason: it's the most pressing topic in security today. This is largely due to a misconception that migration to the cloud will render companies more vulnerable than staying put with onsite data storage. This erroneous paradigm is changing quickly, however—spurred by the costs of inaction when breaches occur, and bolstered by the realities that many companies face as they move to the cloud.

86%

of business leaders are employing a multi-cloud strategy (Forrester)

With nearly 90% of security leaders making the move to the cloud, questions on cloud security should dissipate rapidly–with ample profit and loss incentives to do so.

Migrating to the cloud is simply moving from an existing datacenter to a more secure external one. AWS, Google, and Microsoft offer platforms much more powerful and secure than most legacy options, but it is important to recognize that these platforms will allow almost "anything" installed in the virtual machine. The security model for cloud providers isn't a one-size-fits-all, but rather a shared responsibility model, in which both the business and the cloud provider share security.

In short, the greatest vehicle is ultimately only as good as the driver, tuning, and maintenance schedule. To get the most from a cloud migration, the inherent platform security requires a team of specialists capable of not only maintenance, but also customization and fine tuning (optimization). For example, SoftServe specializes in areas like egress/ingress point security, allowing our clients to have a better analysis of what data is actually moving in and out of their cloud infrastructure. This allows them to dive deeper into their cloud capabilities in a highly customized and optimized fashion.

Cloud security is no fluff

The battle against cyberattacks is real and ongoing—but far better to assess and ensure security prior to release than discover vulnerabilities after the fact. And for legacy software, there's no better time than the present.

Developers generally don't like to work with legacy software for numerous reasons—assumed vulnerability, likelihood of vulnerability, and someone else's work—but net new development is not always an option, or what's necessarily best for the company.

An assessment is key because it's impossible to know where to go or how best to get there without knowing the current state of your software.

There are two prefaces to assessing (and ensuring) inherent security in DevOps:

1. Stop viewing security as a non-functional requirement

2. Insist on agile security practices and tools

At SoftServe, we pride ourselves on being agile and fluid. We recommend the same when building a security culture. Net new development should be inherently secure throughout the process. There are a number of ways to ensure this including: putting developers in charge of secure development, continuous integration security practices in the SDLC, and building user stories.

In addition to the full-time effort teams should dedicate to vulnerability management, security should be inherently built into every project from inception to PoC to launch. For legacy systems, a software security assessment is vital to know the best course of action, and outside expertise should be leveraged if necessary to make it so.

"Only one third of organizations believe they have adequate resources to manage security effectively."

(Ponemon Institute)

Resistance is futile—compliance is mandatory

Security and compliance are often grouped together, but distinguishing them from one another is important. Being compliant, for example, does not necessarily ensure security. But establishing security within compliance is imperative, especially in the wake of new regulations such as GDPR (General Data Protection Regulation).

GDPR is the first wave of a sweeping regulation, but more sophisticated, geographic-specific changes are on the way. This trend may be seen with companies affected by GDPR as well, considering more than half of GDPR affected companies will likely be noncompliant by end of year. In the US, this trend is called a "compliance salad" where different versions of websites are produced based on variable compliance standards from state to state.

Those without adequate resources to manage both security and compliance effectively should seek outside expertise sooner than later. Once a company can check all regulatory boxes, optimizing applicable security is the next step.

At SoftServe, for example, we guide our clients to improve digital maturity and security posture so that when it's time to be certified, the process is streamlined and simple—test preparation if you will. And where multiple contractors are employed, our experts provide redundant verification to ensure the work of others is properly driving certification as well.

Security is in our DNA

Cloud security, risk assessment, and compliance readiness are only a few of the security challenges facing most businesses today. Identifying where your security stands, where it needs to go, and how to get there can literally be a million-dollar question.

Different industries have different regulations that require different preparedness strategies. Sometimes modernizing legacy software is enough, but oftentimes it is not. There is no one-size-fits-all solution in a world where cyber criminals are in a perpetual chess match with developers, ethical hackers, and other security professionals.

SoftServe's methodology for each client and project is secure by design and has been for over 25 years. You have the data and software. We empower you to optimize, secure, and manage it with speed and agility, and within budget.

Start optimizing your security. Contact SoftServe today.

ABOUT US

SoftServe is a digital authority that advises and provides at the cutting-edge of technology. We reveal, transform, accelerate, and optimize the way enterprises and software companies do business. With expertise across healthcare, retail, media, financial services, software, and more, we implement end-to-end solutions to deliver the innovation, quality, and speed that our clients' users expect.

SoftServe delivers open innovation—from generating compelling new ideas, to developing and implementing transformational products and services.

Our work and client experience is built on a foundation of empathetic, human-focused experience design that ensures continuity from concept to release.

We empower enterprises and software companies to (re)identify differentiation, accelerate solution development, and vigorously compete in today's digital economy. No matter where you are in your journey.

Visit our **website**, **blog**, **Facebook**, **Twitter**, and **LinkedIn** pages.

USA HQ
201 W 5th Street, Suite 1550
Austin, TX 75703
+1 866 687 3588

EUROPEAN HQ
One Canada Square
Canary Wharf
London E14 5AB
+44 (0) 800 302 9436

info@softserveinc.com
www.softserveinc.com

softserve