

What's worse than **no** information security?

Thinking you're secure when you're not.

If only Information Security was as simple as adding hardware or installing some patches.

It's easy to think of Information Security tactically — you buy some appliances and tools, hire a security consultant, they review your system settings, check some boxes, deliver a report, and you're done. But as many organizations, both large and small continue to discover, Information Security is a business issue — and solving this issue requires a strategic plan, not a tactical quick-fix. Real and reliable Information Security can only happen if there's a set of business processes in place to support it. You see, true Information Security is a journey, not a destination.

Think about it like this — you can spend a ton of money on security appliances, add firewalls and virus detection systems, you can pass a complete security, privacy, or compliance audit, and then one day an employee finds a thumb drive in the parking lot and decides to see what's on it, or an outside vendor leaves a router unsecured.

This is about to get painful.

We wish we could say this sort of thing doesn't happen, but it does, and what's more these are just two of a vast number of internal and external issues threatening today's organizations. The truth is that if you haven't done a comprehensive assessment of your real risk profile to identify the unknowns, all the security infrastructure and compliance investments you've made become functionally and effectively useless.

"We'd had a consultant come in and perform a review of our technical vulnerabilities. They left us with a list of our security gaps, but we had absolutely no idea how to go forward from there. We contacted AppSec Consulting and they really helped us not only understand our risk profile, but they also helped us plan and build a robust Information Security program to improve our overall security posture."

**JENNIFER J., VP INFRASTRUCTURE
FINANCIAL SERVICES INDUSTRY CLIENT**

Information Security is a business challenge

In our experience, when you start to look at security as a business challenge and not just IT's responsibility, good things start to happen. Information Security in general starts to become more holistic, clear business processes can be defined and implemented, organizations (and the customers they serve) become more secure. And because you're approaching things more strategically, you're lowering your aggregated risk, and winning (and keeping) more business even as your Information Security costs go down and your security reliability levels go up.

So how does a company put Information Security into a business context?

It starts by calling us. For over 10 years we've helped our customers not only meet requirements for ISO 2700x, PCI DSS, HIPAA, SOC 1/2/3, GDPR and Privacy Shield, and more, but we've also helped them develop clear business processes designed to integrate Information Security throughout their entire enterprise and corporate culture, not just one department.

From helping you uncover coding vulnerabilities, to developing policies and procedures that support you as you move forward, our concierge-level services meet the need of businesses of all sizes at every level required.

Our Services

We have a continuum of services designed to fit just about everyone's security needs, and every service we provide comes with a level of experience and focused attention you won't find anywhere else. Our Security Testing team will help you identify the technical issues you should be thinking about, and our Risk Management Team will work with you to develop strategies for addressing them — that means assurance for you, your customers and your partners. And because we're independently owned, you'll find us completely agnostic in terms of the solutions and vendors we recommend — this means you get the solution that fits your needs, not ours.

Security Testing



The most rigorous security testing can only be done effectively by employing highly-skilled human analysis and best-in-class tools. Our proven methodologies consistently uncover vulnerabilities others may have missed, while providing you with a practical roadmap to improve your Information Security program.

- ✓ Penetration testing for web apps, web services, mobile, networks, and physical locations.
- ✓ Application and network security assessments from architecture to code to mobile and beyond.
- ✓ Social engineering and phishing assessments.
- ✓ Design of internal vulnerability management and secure SDLC programs.

Strategic Consulting



AppSec Consulting provides strategic security services designed to help your organization maximize your security, privacy, and risk management investments.

- ✓ Assessment, planning and remediation services delivering a comprehensive strategy for keeping your brand, your systems, and your customers safe. Our services include IT Risk Assessment, strategic planning and remediation roadmapping, security program development, policy development, and security and privacy program and remediation project management.
- ✓ Our tools and assessment methodologies are based on industry best practices, delivered by industry experts.

Compliance Testing and Audit Readiness



AppSec Consulting works with many types of industries, including financial services, ecommerce, healthcare, software, utilities, and hospitality to assist in gap identification and strategic remediation planning for a variety of needs. We work with you every step of the way to make sure you're well prepared, avoiding unwanted surprises during your audit or certification.

- ✓ PCI DSS: advisory, gap assessment, guided Self-Assessment Questionnaire assistance, and Level 1 PCI Report on Compliance audit services delivered by some of the most experienced Qualified Security Assessors in the business.
- ✓ SOC 1/2/3, HIPAA, ISO 2700x, and GDPR/Privacy Shield audit and certification preparation services.

Training



Humans tend to be the weakest link in the security chain. We provide a variety of in-person and Learning Management System-based online training courses designed to help your staff understand how to keep themselves, your business, and your customers safe.

- ✓ Customized training specifically designed to replicate your environment and Information Security challenges.
- ✓ Learning Management tools that can be used for compliance verification and employee tracking.
- ✓ Development of training and awareness programs delivered quickly and cost-effectively.
- ✓ Train-the-Trainer workshops.

One size never fits all.

Every one of our customer's requirements is different and their individual concerns vary significantly, so every project we work on begins with a healthy dose of listening. We pride ourselves on being able to look past what we call "surface security," going deeper to uncover real, day-to-day business risk and exposure. Whatever the issues are, we'll help you identify them and make sure the appropriate people know how to fix them. Most of all we'll help you understand why they happened in the first place, and help define effective policies, procedures, and programs to make sure they never happen again.

Nimble, responsive and focused on you.

Even though we've worked with some of the most recognizable brands on the planet, AppSec Consulting is designed to be nimble. You see, experience shows that the bigger a company in the Information Security space gets, the more they turn into hammers — and we all know that when you're a hammer, everything looks like a nail. We believe this purely tactical, bulldozer approach to Information Security only serves the security provider, not the client; it's difficult to scale and typically full of unseen holes, and the bad guys love that. That's why we stay small and effective, we listen, and we help our clients develop a strategy and roadmap to proactively address current and emerging threats to your business.

This doesn't have to be difficult.

So thinking about your organization, its security and its future — maybe it's time to ask yourself some tough questions — how do you think about security? How does your company as a whole view its Information Security responsibilities? Did your last security or compliance review truly cover all the bases? Do you have business processes in place to help keep your systems, data, and reputation safe? Are your employees and business partners active participants in your security strategy? Are you finding yourself adding more and more appliance and software solutions without a clearly mapped out strategy?

Oh, and do you really know who's on your network right now?

"We'd 'passed' a compliance check with another security company but we still didn't feel like we really knew what was going on our network — We hired AppSec Consulting to take another look. Their approach went far past compliance — they educated our team and helped us set up practical and scalable controls to move forward. I think we're all sleeping a little better at night."

STEPHEN R., CHIEF TECHNOLOGY OFFICER
NATIONAL RETAIL CHAIN CLIENT

It's a lot to think about, but this doesn't have to be difficult. **Give us a call at 408-224-1110, you'll speak with an Information Security expert, not a sales person** —we'll listen a lot, determine your needs, and provide clear, actionable recommendations. We look forward to seeing how we can help.



Information. Security. Handled.™

appsecconsulting.com | 408.224.1110