Justin Armstrong

Masters in Information Security Leadership, Brandeis University, 2018

Certified Information Systems Security Professional
Credential ID: 516453
Issued Feb. 2016

Certified Cloud Security Professional
Credential ID: 516453
Issued March 2024

HealthCare Information Security and Privacy Professional
Credential ID: 516453
Issued November 2022

Member of IEEE SA-P2933 Working Group developing a standard for Clinical Internet of Things (IoT) Data and Device Interoperability

Securing Healthcare

As a Healthcare leader, your pivotal role in steering your organization encompasses a delicate dance between ensuring quality patient care, maintaining a strong and engaged clinical staff, and safeguarding the financial vitality of your institution. Complicating matters, healthcare is under attack, and not just by criminal hackers — as noted in the 2023 Verizon Data Breach Investigations report, your own staff are at the heart of 35% of the incidents.

Justin has worked closely with Executives at Hospitals large and small, and engaged with technical teams on a wide range of IT, Cybersecurity, and regulatory compliance topics. Justin has many years of experience working with Clinicians.

Specific goals Justin will work with you to achieve:

- **Mitigate Risks:** Protect your organization and reduce the impact of enforcement actions by building a Cybersecurity program based on HHS Health Industry Cybersecurity Practices (HICP) and other recognized security practices
- **Preparedness:** Prepare your people — Clinicians, Ancillary departments, and Executives — for a cyber-attack. Going back to paper requires advance planning and practice to be effective. Patient Safety is at great risk, and the long-term health of the Hospital may be at stake.
- **Maximize Payments:** Meeting the requirements of the Quality Payment Program/MIPS and Promoting Interoperability in order to ensure maximum payments.
- **Reduce Fraud:** Build out a Fraud Prevention and Insider Threat program to lessen the likelihood and impact of malicious insiders.
- **Technology Selection:** Select Technologies that will work well in a Healthcare environment and provide measurable improvement.

Our Process

Listen and Understand

It starts with listening. We're not here to tell you how to run your organization — you're the expert.

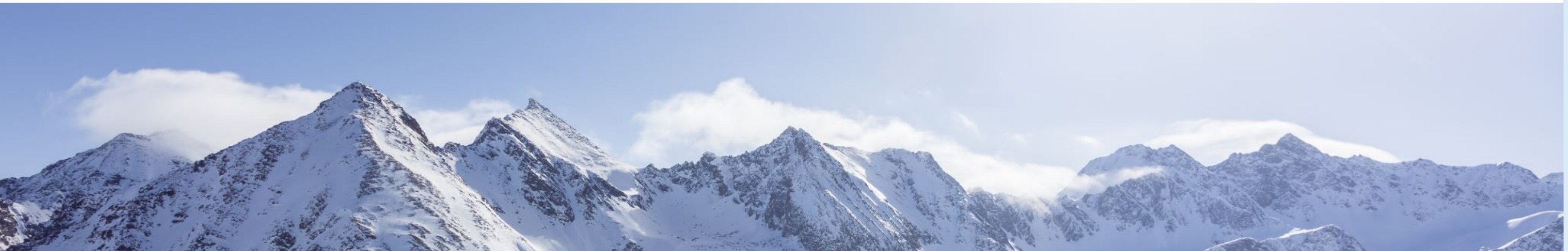
The Security program we build for you will be effective because we put in significant time to understand your business — what matters most, its strengths, and the current threats. We identify security and compliance gaps.

Cybersecurity Sprint

We will perform a gap Assessment against your chosen framework and provide an actionable report with an implementation plan that includes "quick wins" and will help you to make measurable security improvement in a short time.

The Marathon: Strategy

The core practice of Information Security is to perform a risk assessment and to create a risk treatment plan based on the top risks which were identified. While the gap assessment may take a few months to implement, the risk treatment plan typically requires a year or more.



Part of Your Team!

We don't create a plan and then leave you to implement it. We are with you every step of the way. Here are a few examples:

- **Building a "Security Culture":** This requires regular engagement with people at all levels of your organization.
- **Project Management.** If we are helping you achieve your ISO 27000 series certification or managing your SOC 2, we are there working with your team day in and day out – keeping the project on track.
- **We are there for you when you need us** – whether a contract requires review from a security perspective, or a client has questions about your security stance.
- **Incident Response Planning:** We spend a significant amount of time working with your team to prepare an effective plan that is clear, adaptable, and realistic. *More importantly, the work we do with your team is what makes the plans effective.*
- **Incident Response Tabletop Exercises:** We build and coordinate exercises which encompass multiple teams – clinical staff going back to paper, IT managing the infrastructure, and executives managing the message.

Let Us Build Your Security Culture

In Aviation, Healthcare, and other sectors, you often hear about building a strong "Culture of Safety." This is one of the highest priorities for organizations which can impact human life. Building a culture of safety is seen as foundational. Without it, human lives will be lost.

The same goes for cybersecurity. With the great increase of threats, it is no longer adequate to educate people about the basics. There needs to be a strong culture of security. Everyone needs to feel free to speak up when they see something wrong or make a mistake.

Build a Security Culture

Your people are your greatest asset against cyber criminals, but only if they feel free to come forward whenever they make a mistake or notice something that seems off. Building a security culture is not easy – it will take time to educate your people, modify behavior, and convince them that the organization is committed.

Why Watching Security Awareness Videos Doesn’t Work

Your people are busy. They are diligent. When security awareness videos are required viewing, no doubt many of them simply put the video on play and get back to their work! Even if they do give the video their full attention, it’s passive. They are not being asked questions. They are not being compelled to stop and think. And thinking is exactly what we need them to do. Criminals are craftier than ever before. With the help of AI and deep fakes, they can be quite convincing! Gone are the days of the phishing emails with poor English.

Engaging Presentations With Real Stories!

People love a story – it makes it real; it is relatable. We use stories from personal and professional life to illustrate key points. We ask questions to help people learn to think through these types of common scams. We foster the correct environment by speaking in a non-judgmental way.

It’s Personal!

We provide everyone with helpful tips they can use in their personal life. When your people learn how to securely shop and bank online, they are learning important skills which they will also apply in the workplace. We also build trust so that they will come feel free to come forward and ask questions. We can also work with your help desk or IT team so that they can learn how to build this reservoir of trust.

Interactive

We work hard to make our sessions interactive. For example, we will walk the through an important process so that they see it is easy to do. It is vital that we overcome the intimidation factor. For example, we show them how to unshorten those notorious shortened links and have them try it right during the session.

Making It Stick

To make this stick, we will work with you to go beyond the annual training by providing posters, monthly emails, swag as rewards for the most security conscious people, and more.

Incident Preparedness

Business Continuity, Disaster Recovery, and Incident Response

Incidents happen all of the time. They vary in type and impact. As we saw with the Crowdstrike outage (July 19, 2024), it's not always a cyber-attack. While I have been involved with nearly 100 ransomware incidents, I have also seen a wide variety of problems ranging from Squirrels bringing down the power grid to serious bugs in Microsoft updates.

Incident preparedness goes beyond the creation of incident response policies, procedures, and playbooks. **It's a process!** Key stakeholders from across the organization must be involved. The process itself has great value. Critical systems and processes will be identified, and contingency plans created. The stakeholders will learn to collaborate together so that they will function as a team when an incident does occur.

Organizations with a well thought out and tested plan respond more quickly and minimize damages and costs. We will work with your executive team on Crisis Management and communications so that they understand clearly how to manage the message.

In addition to advance planning, we will work through detailed tabletop exercises with you and your team since “no plan survives first contact with the enemy.” This includes strategies and tactics for the clinical, administrative, IT, and Security teams.

Incident response tabletop exercises will exercise all parts of the plan – clinician ”back to paper” procedures, IT response to a cyber-attack and numerous other types of emergencies, and managing both internal and external communications.

“Plans are worthless,
but planning is everything”
attributed to Dwight D. Eisenhower

Regulatory Compliance and Privacy

Meet Compliance and Privacy Requirements

Keep regulators happy and avoid hefty fines and corrective action plans.

- HIPAA
- FDA Medical Device requirements
- SEC Cybersecurity Disclosure Rules
- PCI DSS
- The GPDR
- FERPA, COPPA
- CCPA/CPRA and other State Privacy Laws
- Canadian Privacy Regulations

Comply With SEC Cybersecurity Disclosure Rules

Wondering how to conform to the new SEC rules on cybersecurity disclosure?

We will not just craft your cybersecurity incident disclosure policies and procedures, but work with you to develop a 10K statement on Cybersecurity Risk Management which strikes just the right balance.

As part of the engagement we can work with you to improve your Cybersecurity Risk Management, Governance, and Board Reporting.

QPP/MIPS/Promoting Interoperability

Meet requirements through these services:

- Security Risk Analysis (SRA)
- Secure deployment and management of your REST API infrastructure
- Clear guidance on managing third party apps connecting to your EHR
- Implementation of the SAFER guides

Privacy

- Gap Assessments
- Data Privacy Impact Analysis
- Policies and Procedures
- Privacy by Default and by Design

Enable Business

In today's business landscape, the demands of prospects, loyal customers, and valued partners are evolving. There is a growing emphasis on security and privacy. Meeting these evolving expectations is paramount to the success of your business.

Protecting Your Reputation

Keeping you out of the news — security keeps your organization off the front pages for negative reasons.

Reassure Your Customers

When a system similar to yours is hacked, the security team can provide details to your customers on how your product is secure, or provide updates and techniques for securing it.

Encourage Investment

Now more than ever, investors are looking for information about your cybersecurity risk management and governance!

Smooth Sailing

Smooth out the sales process, increasing the speed of business.

- Achieve ISO 27001 certification
- Receive a clean SOC 2 Audit
- Build out a library of RFP responses for security, privacy, and compliance questions
- Create a Security and Privacy whitepaper for your prospective clients
- Educate your Sales and Marketing team

Contract Review

Whether it is a contract with a customer or a vendor, cybersecurity clauses are written into contracts so that all parties clearly understand the responsibilities and expectations of each party.

More than once, I have seen prospective customers try to slip in cybersecurity language that is misguided and heaps liability on the vendor.

SOC 2 and ISO 27001

Navigating the complex landscape of SOC 2 and ISO 27001 compliance can be challenging. We facilitate the process by:

1. **Listening first!** We work to understand your business, its unique challenges, and the culture.
2. **Strategy —** Providing your executive team with a clear roadmap up front so that adequate resources are committed.
3. **Engaging** directly with management and front-line staff to establish clear policies and procedures that fit your culture.
4. Building your **Policies, Procedures, Risk Management process, Third Party Risk Management program, and more.**

Secure Your Products

Secure Software Development

Justin worked as a Developer on many major projects at MEDITECH, developed and established coding standards, led code quality initiatives, and led Product Security for 6 years.

Justin will work with you to build out your product security program, including:

- Building a culture of security within your Development and Engineering teams
- Open Source Software management - guidance on licensing and technical review, creation of policies and procedures, education
- Technical recommendations on automated security scanning and open source software vulnerability management
- Specific guidance on such frameworks as the NIST SSDF, BSIMM, and OWASP SAMM
- Technical recommendations for web applications and REST APIs
- Threat modeling of Software and Systems

Protect Your Intellectual Property

Once your IP is gone — it is gone. Protect it now before it is too late.

Justin Armstrong will educate your executives and staff on the current threats from China and other nation states, and provide specific actionable steps you can take to secure your IP.

Contact us now for a free consultation.

www.ArmstrongRisk.com