secure by design

Building A Secure Product From Day One

engineered innovation group

TRAVA

In the rapidly evolving world of technology, security, privacy, data retention, and compliance are crucial components of any software product and business.

It can be challenging to consider these needs fully while building your Minimum Viable Product (MVP) and establishing your business. However, making strategic, sound decisions early in your product's life can save enormous time, money, and effort as you grow and position you to win business.

Security and privacy programs encompass both the product and the organization, including policies and procedures. Policies define what is expected, while procedures explain how to implement them.

Some key policies that you should include are acceptable use, clean desk, privacy, data breach, business continuity, and risk management.

TABLE OF CONTENTS

Developing an MVP

At Engineered Innovation Group, we approach security with our prospects and clients in partnership with Trava Security, a cyber risk management and insurance platform. Our approach involves several steps, starting with awareness and appreciation.

AWARENESS & APPRECIATION

During the pre-build stage, it is essential to have a general awareness and appreciation for the need for privacy, compliance, and security. This includes setting aside a budget for future security needs in your business plans and identifying the internal owner for security, privacy, and compliance. In the early stages, this is often the Chief Information Officer (CIO) or Chief Technology Officer (CTO).

ASSESSMENT & CURRENT STATE

Once building begins, there is a constant need to assess your privacy, security, and vulnerabilities. This can be done through a mix of tools, like Trava's comprehensive risk and vulnerability assessment tool partnered with security expertise and vCISO services. Regular evaluation of the privacy and data compliance needs is critical when collecting and leveraging new data in your platform. Additionally, you will need to establish if and when any specific certifications will be required as part of your go-to-market strategy when working with early customers or having prospect conversations.

ROADMAP: STRATEGIC & DIRECTIONAL

Building a security roadmap can only happen once you understand the assessment and current state. From this point, building out a formalized roadmap that is both strategic and specific in the near term and directional in the long term can be helpful for internal alignment, resourcing, and planning.

BUILDING: SECURITY & COMPLIANCE

When building your product, there are some steps you need to take to ensure that your product is secure and compliant. These steps include creating an information governance policy and a privacy policy. The information governance policy outlines how information is stored, used, and accessed within the organization. The privacy policy outlines how you handle customer data and their right to privacy.

By following these steps, you can build a secure and compliant product from day one. It is essential to take these measures seriously and prioritize them in your product development process to save time, money, and effort in the long run.

Starting a Cybersecurity Program

In today's digital age, cybersecurity threats have become increasingly sophisticated and prevalent, making it more critical than ever to establish a robust cybersecurity program. Such a program can help organizations safeguard their sensitive data, maintain regulatory compliance, and prevent costly cyber attacks. However, building a comprehensive cybersecurity program can be a daunting task, requiring a thorough understanding of the organization's specific objectives, potential risks and vulnerabilities, and the necessary technical and administrative controls. To help organizations establish an effective cybersecurity program, key steps are as follows:

- **Define Your Objectives**
  Identify the specific goals and objectives for your cybersecurity program, such as protecting sensitive data or ensuring compliance with regulatory requirements.

- **Conduct a Risk Assessment**
  Assess the potential risks and vulnerabilities that your organization faces, including both internal and external threats.

- **Develop a Cybersecurity Policy**
  Create a comprehensive cybersecurity policy that outlines the procedures and best practices your organization will follow to mitigate and respond to cyber threats.

- **Implement Security Controls**
  Implement technical and administrative security controls to protect your organization's assets, including firewalls, anti-virus software, access controls, and employee training.

- **Monitor and Analyze Security Data**
  Collect and analyze data from security tools and systems to detect and respond to security incidents in a timely manner.

- **Establish Incident Response Procedures**
  Develop a plan for responding to security incidents, including steps for investigating and containing the incident, as well as procedures for notifying relevant stakeholders.

- **Continuously Improve Your Program**
  Regularly review and update your cybersecurity program to address emerging threats and to ensure that it remains effective in protecting your organization's assets.

What is Security vs. Privacy vs. Compliance?

In today's digital age, cybersecurity is a critical consideration for any business that collects and processes sensitive data. As companies grow and expand, they need to assure their enterprise customers that they have strong information security protocols in place. In this context, three terms often come up: security, privacy, and compliance.

- ☑ **Security refers to the measures put in place to prevent unauthorized access, use, disclosure, or modification of data.**
- ☑ **Privacy concerns the collection, use, retention, and disposal of personal information in accordance with established ethical and legal principles.**
- ☑ **Compliance is the adherence to industry-specific regulations, standards, and best practices aimed at ensuring security and privacy.**

Many small and medium-sized businesses make the mistake of assuming that being cybersecurity compliant is the same as being secure. However, compliance is just one aspect of a comprehensive cybersecurity program. In this section, we'll delve deeper into the difference between security compliance and cybersecurity, why both are crucial and how businesses can achieve both.

SOC 2 Attestation & ISO 27001 Compliance

SOC 2 attestation and ISO 27001 certification are recognized standards that companies must accept if they are going to sell their services to enterprise-scale customers. These standards demonstrate that a company's systems are set up to ensure the security, availability, processing integrity, confidentiality, and privacy of customer data. They are particularly relevant to cloud-based Software-as-a-Service (SaaS) providers. The compliance process requires a team that can assess an organization's current state against either the SOC 2 or ISO 27001 standards and identify any gaps in policy, process, people, and technology. Once gaps are identified, a comprehensive plan must be developed to close those gaps in a timely manner in order to meet the certification deadline. The process can be overwhelming for small business leaders because it requires very specific controls to be implemented in a certain way, as documented by detailed evidence.

While achieving SOC 2 attestation or ISO 27001 certification is certainly important to assure customers and clients that they have data protection protocols in place, it is not the sole indicator of being cyber secure. Certifications alone will not mitigate the risk of a cyberattack.

Comprehensive Cybersecurity Strategies

A comprehensive cybersecurity program should go beyond compliance and include measures to identify and mitigate risks on an ongoing basis. Every company is different in terms of cyber maturity, the number of employees dedicated to cybersecurity, and the financial resources to invest. However, here are three integrated steps to building a complete cybersecurity program

UNDERSTAND RISK

Running vulnerability risk assessment scans should be on a frequent and ongoing basis. Organizations that scan with a steady cadence remediate flaws on average 15.5 days faster. Types of scans include the dark web (frequent), internal and cloud environment scans (weekly), and external scans (monthly).

MITIGATE RISK

Once you understand your risk with regular vulnerability assessments, the next step is to mitigate the opportunities for cyber threats by prioritizing according to risk severity and repairing the most severe areas of vulnerability. Most scans produce results that are referred to by their Common Vulnerabilities and Exposures (CVE) designation.

TRANSFER RISK

Cyber insurance allows businesses to transfer residual risk in case of a cyberattack. This allows companies to recover financial losses from business interruption, among other types of business protections.

To summarize, being compliant is important to giving your customers confidence that you are protecting their data, but it is not the same as being cyber secure. A comprehensive cybersecurity program should go beyond compliance and include measures to identify and mitigate risks on an ongoing basis. By understanding, mitigating, and transferring risks, businesses can build a comprehensive cybersecurity program that protects sensitive data and ensures business continuity in case of a cyberattack.

Industry Considerations & Certifications

Specialized security certifications may be table stakes in some industries, while in others, you will be able to scale and grow without these formal certifications.

Here are a few acronyms and regulations we often work with our clients on building a security roadmap towards.

- **HIPAA**
  is a United States federal law that regulates the privacy and security of protected health information (PHI).
- **ISO 27001 Compliance**
  is a globally recognized standard for information security management systems (ISMS) that requires organizations to establish, implement, maintain and continually improve their security practices.
- **GDPR and CCPA**
  are data privacy regulations, with GDPR covering the European Union and CCPA covering California, USA, that require companies to protect and manage personal data of their users.
- **SOC2 Type 1 and Type 2**
  are audits that assess the effectiveness of a company's internal controls and their ability to safeguard customer data.
- **CMMC, or Cybersecurity Maturity Model Certification**
  is a cybersecurity standard that assesses the ability of defense contractors to safeguard controlled unclassified information (CUI) and Federal Contract Information (FCI).

Right Size & Timing

It’s critical you right-size your early security and privacy investments—what’s the right approach and timing for one company is likely slightly different for you. Engineered Innovation Group and Trava Security can quickly provide a right-sized security roadmap to ensure you invest the right amount of your capital and energy into security.

engineered innovation group

Engineered Innovation Group (EIG) builds MVP products for venture-backed startups. We build software while also building out product and engineering organizations alongside founders. Our ability to grow junior engineering talent and our use of technology to expedite early-stage product development set EIG apart from other design agencies and dev shops—and keep our rates palpable to startups. Our services span all domains of a highly functioning software company, from software engineering to security programming to product design.

Contact EIG

TRAVA

Trava was founded by Jim Goldman and Rob Beeler to protect businesses and insurance agencies from the potential damage of cyber threats. By integrating risk assessment, risk mitigation, and cyber insurance renewal preparation into one, convenient, comprehensive cyber risk management platform, Trava enables business owners and IT professionals to operate secure, productive businesses without fear of interruption or loss caused by cyber incidents.

Talk to Trava