Growing a Technology Company Using a Secure-by-Design Approach

In 2018, Trigo Vision was founded by brothers Michael and Daniel Gabay to help grocery stores embrace digital transformation and innovate toward a checkout-free experience for customers. The start-up, based out of Herzliya, Israel, built a technology predicated on machine learning (ML) and computer vision that anonymously tracks shoppers, detects their in-store interactions with products and automatically creates a shopping list with the associated price. When the customer leaves the store, they receive a detailed receipt of their purchases. This technology allows customers to use their personal mobile phones to pay as they shop without any scanning requirements or long periods waiting in checkout lines. The brothers' vision for the product was similar to Amazon Go (also founded in 2018) but intended for use in any retail environment.

From the beginning, information security was always going to be a consideration; predicated on a tracking methodology and the collection of everything from biometric data to personally identifiable data and financial data—from both a consumer and a retailer perspective. In short, Trigo needed to build hardened cybersecurity into its design.

A cybersecurity team is not often a significant part of such a young company's plan; however, the executive team, along with its investors and board of directors (BoD), knew that Trigo needed to focus on securing its internal infrastructure and the product it delivered and installed in retail environments. Because the product is built to be deployed by major retailers across potentially hundreds of retail stores globally, preventing a data breach or even a reportable security incident is extremely important. Trigo's first customers and early adopters expect no less than enterprise-level security, even though Trigo is a nascent start-up.

Thus, in March 2020, closely following a second round of funding, Trigo hired its first cybersecurity executive, Koby Zvirsh, as the company's information security manager whose charge was to lead internal security and product security.

At the time of this writing, Trigo is a three-year-old company and employs 100 people, with the bulk of the staff working on research and development (R&D). As the only cybersecurity professional, Zvirsh is responsible for all aspects of information security, including, but not limited to, the product, the company's infrastructure, the corporate environment (e.g., laptops, in-office devices, mobile phones) and security for Trigo's cloud environments. Customers and prospective customers routinely require Trigo to complete security and privacy questionnaires before testing the product, and the EU General Data Protection Regulation (GDPR) and similar international data protection regulations are top of mind for the company and its customers.

With strong backing and support from the executive team, Zvirsh has been on a mission to ensure that Trigo is setting the foundations for world-class cybersecurity processes now, despite its small size, so that as it grows, the company can evolve to a best-of-breed, secure-by-design enterprise. Relying on his experiences working in larger organizations and at a leading cybersecurity solutions provider, Zvirsh joined Trigo to make an impact and help build security from scratch.

Challenge

Like other software providers, Trigo's main cybersecurity challenge is its need to achieve a high

KATIE TEITLER

Is a senior product marketing manager at Axonius where she is responsible for the company's cybersecurity asset management product messaging. She is also a co-host on the popular podcast, Enterprise Security Weekly. Prior to her current roles, Teitler was a senior analyst at a small cybersecurity analyst firm, advising security vendors and end-user organizations and authoring custom content. In previous roles, she managed, wrote and published content for various research firms including MISTI (now part of the CyberRiskAlliance), a cybersecurity events company; and was the director of content at Edgewise Networks, now part of ZScaler.

level of security—for both its internal systems and its product offering—while being a start-up. Though the company is dedicated to building a secure offering, it is unusual for such a young company to have a dedicated, in-house security resource (though, thankfully, it is becoming less so over time). In addition, as a start-up, while the company has the backing and support of the executive team and the investors, there is no established security program from which to build; it is starting from scratch, which is a challenge, but also has its benefits. Building a security program and culture is difficult for any organization, but especially at one with a single dedicated security professional and a product going through rapid development.

Further, the enterprise feels it cannot afford even one small breach or moment of bad publicity due to the highly sensitive nature of its product offering and the reputation of the clients it serves, yet the product must be useable and user friendly, which poses well-known challenges to building a secure-by-design company and product.

Securing Corporate Infrastructure and the Production Environment

Within Trigo's corporate infrastructure, all technologies must be deployed, configured, managed and maintained securely. Because the IT infrastructure is so vast and spans traditional operational technology and software development tools, Zvirsh cooperates with three of Trigo's IT—not security—experts. They act as support for the security program, relying on Zvirsh's expertise.

For instance, Trigo has always had a bring-your-own-device (BYOD) program, which is commonplace in today's workplace but is not without IT obstacles. Therefore, Zvirsh has spent a considerable amount of time working with the IT department and speaking with executives, explaining why mobile security must be part of the BYOD program and emphasizing that BYOD should be more than a perk for employees. Even though Trigo is a young company, Zvirsh has convinced the senior team that every approach it takes should be based on what would be implemented in a larger enterprise, similar to those at which many of the team members worked prior to joining Trigo.

What this means is that Zvirsh plays the roles of security professional, trainer and security product manager, explaining and demonstrating mature security processes for corporate systems and software development production environments. This cuts across disciplines, be it mobile, laptop, server, cloud or product.

At this stage in its evolution, Trigo's team knows that it cannot accomplish everything a large enterprise would in terms of cybersecurity processes and technologies, and so it must be selective with its efforts. Zvirsh constantly pushes for advancements with the security fundamentals that will have the greatest impact, for instance, implementing least-privilege access.

Another hurdle for Trigo was the dramatic and instantaneous shift to remote work that occurred in March 2020. While Trigo regularly issues corporate-managed laptops, which means employees could transition easily to home-based work, the company did not have any controls in place to facilitate a secure remote workforce. With support from leadership, Zvirsh relied on his previous enterprise-level experience to roll out secure access, ensuring that least-privilege permissions were correctly configured and settings and policies abided by the most rigorous standards, whether for the corporate network and resources or for production environment tools and technologies.

> "Trigo's main cybersecurity challenge is its need to achieve a high level of security—for both its internal systems and its product offering—while being a start-up."

As a newer company, Trigo does not maintain any on-premises infrastructure, but that meant Zvirsh and the IT team had to meticulously evaluate and adjust all cloud and virtual settings, configurations and access controls one at a time, and each employee's laptop controls and permissions.

> "Trigo also leverages the security requests of larger customers and prospects, as these are prioritized in the product development cycle since they are attached to company revenue and growth."

Solution

When building the security program for Trigo, Zvirsh's approach was to build the baselines as if he were doing so for a large, amply resourced enterprise. Given the growth Trigo had already seen in such a short time and that which they expect in the coming years, the company's advisors, investors and cofounders agree that this is the right approach. To create these building blocks and aim for enterprise-level security for Trigo, stakeholders are working on fostering strong relationships and collaboration between Zvirsh and the IT team. The two teams continuously discuss how security features must be integrated with the product and internal or cloud-based systems and infrastructure. This includes security-focused policies and support from legal teams to ensure compliance with applicable laws and regulations.

Trigo also leverages the security requests of larger customers and prospects, as these are prioritized in the product development cycle since they are attached to company revenue and growth. But Zvirsh realizes that the security program does not trump all other product improvements and product development processes; though the company and its advisors recognize the importance of information security, ultimately, security is a business risk that the company must manage at a holistic level. Therefore, Zvirsh considers his role to be one of an advisor, helping the company learn and understand how a best-of-breed program would operate and then giving decision makers alternatives to align with the company's capabilities when best-of-breed is out of scope at its nascent stage as a start-up.

Collaboration

Gaining cooperation and buy-in for cybersecurity requires a good deal of awareness and education. To achieve this, Zvirsh leverages his personal experience, but also relies on the company's ever-growing support for, and acceptance of, security best practices. For this endeavor, Zvirsh has enlisted the help of the company's procurement head. Together, they agreed that all IT acquisitions must involve a security review (**figure 1**). This process guarantees that the security team is aware of all technology purchases and deployments and can supply recommendations for secure configuration and management. As a result, each technology implementation is reviewed to ensure that security standards are met, and that the data collected, stored and processed are compliant with major data security and privacy regulations.

Security Awareness and Training

For security to remain top of mind, Zvirsh periodically discusses security topics with the executive team, such as software vulnerabilities, phishing attempts and ransomware attacks. The goal is not to scare the executive team into supporting security, but to make sure it is aware that cyberattack threats are real and something with which the company must contend, especially as it grows.

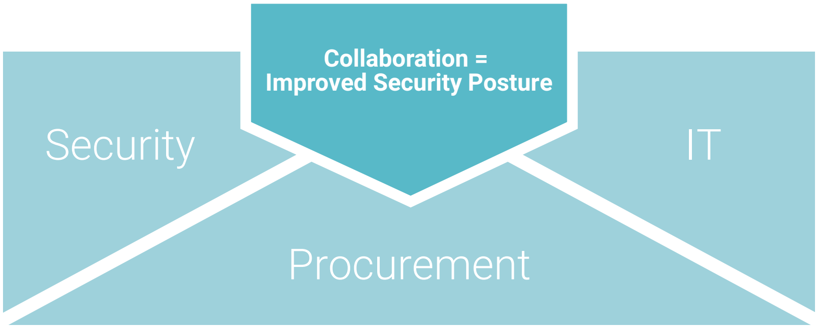
More formally, the company has approved and conducted security awareness training with simulated

LOOKING FOR MORE?

- Read *Governance Playbook: Integrating Frameworks to Tackle Cybersecurity. https://www.isaca.org/governance-playbook-integrating-frameworks*
- Learn more about, discuss and collaborate on information and cybersecurity management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 1

Security, IT and Procurement Collaboration



phishing campaigns that measures employees' levels of awareness and actions (**figure 2**). As a result, click rates on suspicious and malicious emails have decreased steadily over time. Further, employees are encouraged to report any suspicious emails and receive positive reinforcement for forming good security habits. Zvirsh set up a dedicated inbox for reporting potential phishing attempts and a Slack channel through which employees can ask security questions and communicate concerns, and employees are welcome to use various other messaging channels such as WhatsApp for reporting, making it easy and convenient for them to contribute to good security hygiene and improve the company's overall security posture.

The human factor has a significant impact on success, Zvirsh says, and the company has approved future all-hands security training for employees and dedicated security training for its developers in particular, the largest group in the company and the team responsible for the secure deployment and maintenance of Trigo's customer-facing product. The goal is to enhance security skill and mindset and improve Trigo's security posture regardless of its size.

FIGURE 2

Trigo Vision's Integrated Security Training and Awareness Program

In addition, Trigo will begin to run third-party penetration (pen) tests against its product and infrastructure to identify and address any security vulnerabilities and demonstrate a hardened security posture. The company is also evaluating security certifications that it can obtain to show its dedication to information security and differentiate the company and product from potential competitors. Zvirsh says that the team wants to be able to demonstrate security-by-design to ensure that customers have the highest level of confidence in the product and company.

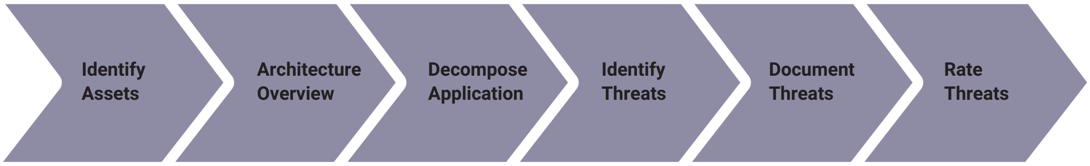
Framework-Based Risk Management

Trigo leverages industry-leading risk management frameworks to implement security controls, but Zvirsh says the organization wanted to take a differentiated approach to risk management. The enterprise focuses on threat modeling rather than risk alone, so that identified risk has greater relevancy to Trigo's environments. The real-life risk scenario moves the company away from the checklist mentality that is common among organizations with lesser security focus and gives Trigo a clear and efficient path for handling risk sources and threats.

Trigo currently uses the concept of threat modeling (**figure 3**) and a risk register for software development and for internal systems. This helps the development team prioritize any identified vulnerabilities in the product, but does so in a way that integrates with its DevOps approach. As such, security is baked into the developers' work processes and guarantees that any identified bugs

FIGURE 3

Threat Modeling Process



are handled in a timely fashion, without slowing down development. Engaging with the DevOps team in this way solves many problems of vulnerabilities deployed into production and helps create a positive perception of security as an enabler rather than a hindrance.

Another solution Zvirsh has used to improve Trigo's security is to leverage customers' external benchmarks and scorecard ratings. When Trigo rates well, Zvirish uses the results to evangelize the impact of mature security processes. The company can also use the results to demonstrate its commitment to a top-rate, secure product and gain more customers.

Tools

Because software development is at the center of Trigo's purpose, one of the most important areas for vulnerability management is code scanning. Zvirsh has enlisted application security scanning for software being built and deployed a cloud configuration management tool for the development environment. Zvirsh needed to justify the expense and processes to implement these solutions but felt that explaining the risk in business terms made it a simple conversation. For instance, Zvirsh speaks with the executive team and the company's advisors about how a breach would negatively impact the company's ability to operate in terms of production (e.g., engineers would have to divert focus from building a product to remediating bugs that were not attended to during the build phase), sales (e.g., retailers might be reticent to sign contracts with a company that has been breached, especially if the breach can be traced back to insecure design) and brand reputation (e.g., customers might not want to download and use an app that has leaked private data, putting those data in the hands of malicious actors).

In addition, because the company must remain nimble, and because security is currently a one-person team, security tooling needs to provide quick results and cannot require a lot of tuning. Trigo also uses standard IT monitoring and security tooling, despite being a small company, including security information and event management (SIEM), a next-generation firewall, intrusion detection systems (IDS)/intrusion prevention systems (IPS), web filtering, native controls within certain IT environments, and a number of reliable open source security products. Zvirsh and the IT team are making good use of what is available and building upon that, when possible, to achieve enterprise-level security.

Secure Access

In the wake of the 2020 work-from-home movement resulting from the COVID-19 pandemic, it was necessary to implement a secure access policy. This became more important when the organization transitioned to a hybrid work structure. Fortunately, all employees were already issued corporate-owned laptops, but mobile devices were personally owned. Nonetheless, Trigo's executives decided to require a mobile device management (MDM) solution for all mobile devices requesting access to enterprise resources. At first, employees were resistant, concerned about privacy and monitoring of their nonwork-related activities. After detailed discussion, employees were educated about the technology, told what it would and would not be used for, and reassured that implementing MDM was not only a benefit for the company, but also served as protection against cyberattacks. Zvirsh wanted to implement MDM quickly, but he also wanted people on his side, and understood that the company would be better off if he could gain buy-in rather than force it.

The keys to implementing security solutions at Trigo are education and collaboration, employee feedback, guidance, and expert advice.

Benefit

A more mature cybersecurity program will help improve the product and customer experience. Trigo's deployment of the product will drive revenue, which, in turn, will generate funding for its cybersecurity program. One of the challenges for Trigo's security team is proving that the enhanced security program has aided primary business objectives. Based on the early successes Trigo has seen thus far, the executive team and advisors are cautiously proceeding with security team advancements.

Zvirsh's collaborative and educational approach has benefitted the company in many additional ways, well beyond security. The relationships he has built

> "Because the company must remain nimble, and because security is currently a one-person team, security tooling needs to provide quick results and cannot require a lot of tuning."

with commercial vendors have allowed him to rely on his solution providers as extensions of his team. They reach out to him proactively about product enhancements and feature/functionality updates.

Furthermore, these collaborative efforts have improved working relationships within the company and helped grow a culture of security from an early stage. The benefit is a companywide security mindset and the support to be creative when certain security processes or tools cannot yet be implemented. In turn, Zvirsh understands that product development and customer service reign supreme and that his actions must support the enterprise's overall strategic goals. Even as a company in its early stages, the return on investment so far—both in terms of security spend and the time and effort spent on education and relationship—is high.

Results

With continuing support from management and the right approach to building a security program, even with a one-person team, results have emerged.

Leaders across the company, from executives to team leaders, have begun to recognize the importance of a dedicated security function.

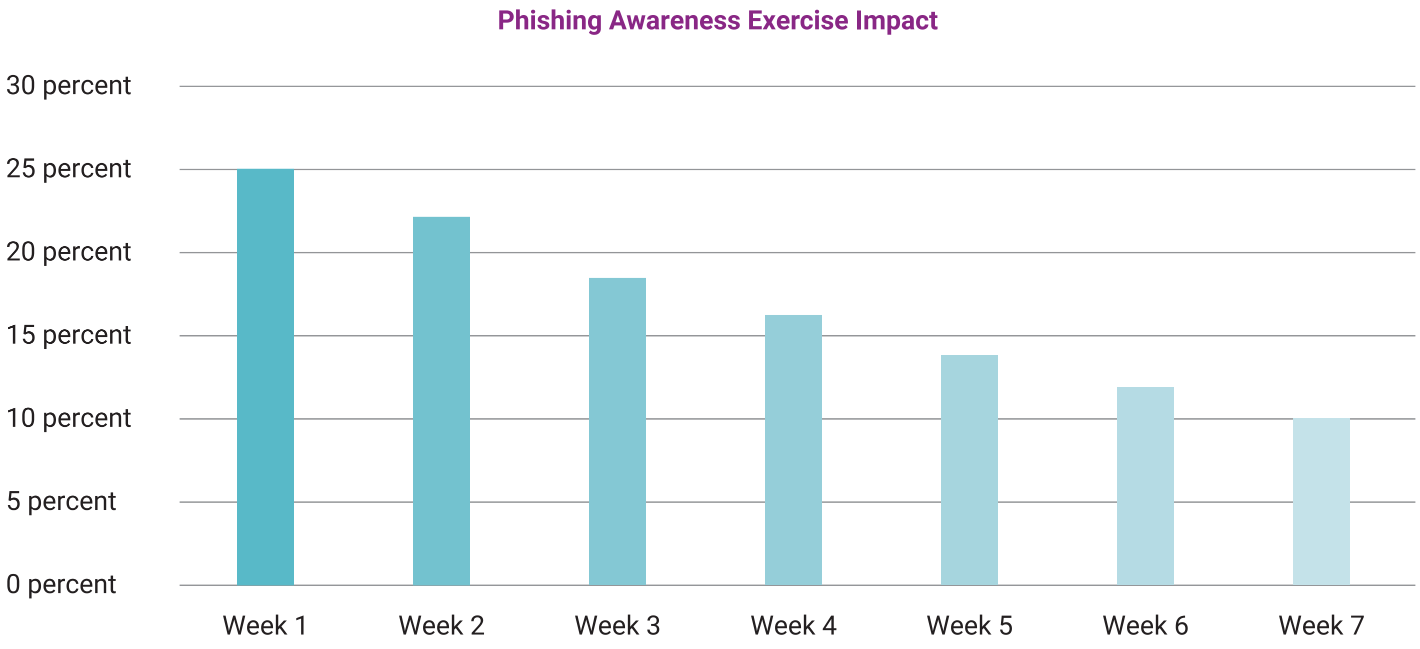
Following a phishing awareness exercise, click rates on simulated phishing URLs went from 25 percent to 10 percent in a matter of weeks (**figure 4**). In addition, employees have started reporting suspicious emails (real, not simulated) at a higher rate.

As part of Trigo's third-party, Software-as-a-Service (SaaS) security standards, Zvirsh has required compatibility with the company's single sign-on (SSO) tool. Today, more than 90 percent of the SaaS services Trigo uses are federated through the corporate SSO, meaning that less manual effort is needed for authentication. In addition, it adjusted the configuration to allow a true SSO user experience even when employees are working remotely. This has resulted in a decrease of the authentication prompts from two or three to only one set of user credentials. This is an improvement because, from a security perspective, there is less risk of man-in-the-middle (MitM), credential stuffing or other forms of credential compromise. From a user perspective, it is less likely that a user will be locked out and, thus, require assistance from the help desk.

In addition, a cloud security posture management (CSPM) tool was deployed so that Zvirsh has full visibility into Trigo's cloud deployments and better control over remediation of vulnerabilities

FIGURE 4

The Impact of Security Awareness Training on Simulated Phishing Click Rates



in the environments. Before the CSPM tool, Zvirsh had to use three disparate tools specific to each environment; now, he has uniform visibility and control from one dashboard, with improved reporting and uniformity across cloud environments.

Trigo has also achieved a reduced mean time to remediate bugs based on the results of pen testing and the formation of a quality assurance (QA) team within the development team that helps triage software bugs.

Conclusion

Start-up enterprises are often resource challenged, meaning they have to make difficult budgetary and staffing decisions in exchange for planning, building and bringing to market a viable product or service. Trigo Vision's founders and investors understood early on that that its product, a computer vision tool that enhances consumers' shopping experience, is predicated on strong cybersecurity foundations. As such, they quickly identified a need to "bake" security into the product but also understood that security had to be built into the company's internal operations as well. By hiring a full-time security employee with experience at larger enterprises, Trigo Vision was able to implement security controls from the get-go and can now iterate on security best practices as it grows. In turn, the company's lack of security incidents helps it generate revenue quicker, which will support additional security best practices and controls in the future.

One of the main drivers of Trigo's success has been communication. Trigo's security lead, Koby Zvirsh, regularly communicates with the founders and advisors about including security in the company's internal systems as well as the product offering.

Other key elements of Trigo's security success include (**figure 5**):

- **Increased collaboration**—Zvirsh has recruited the IT teams and procurement department to help with security hygiene and best practices.
- **Security training and awareness**—Because the founders and advisors understood early on the importance of security being baked into the fabric of the company, Zvirsh has been able to conduct regular training with employees and, as a result, the company has seen a decrease in successful phishing attempts and an increase in good security practices by employees.
- **Implementation of risk frameworks**—Trigo uses threat modeling and a risk register to identify and then manage cybersecurity risk.
- **Secure development**—Through constant communication and improved collaboration, Zvirsh has been able to work with software development teams and teach them about the benefits of secure development, ensuring a hardened product and increased sales opportunities.

FIGURE 5

Key Elements of Trigo's Security Success

Element	Benefit
Communication	Ongoing discussion about including security in internal systems and the product offering.
Increased Collaboration	IT teams and the procurement department have been recruited to help with security hygiene and best practices.
Security Training and Awareness	Regular training with employees has been conducted and the organization has seen a decrease in successful phishing attempts and an increase in good security practices by employees.
Implementation of Risk Frameworks	Threat modeling and a risk register are used to identify and then manage cybersecurity risk.
Secure Development	Constant communication and improved collaboration with the software development teams educates them about the benefits of secure development, ensuring a hardened product and increased sales opportunities.