DIGITALLY REMASTERED

Integrating Security to Fuel Your Transformation

When every business—be it a startup or stalwart—is connecting with customers through software, it becomes imperative to deliver new experiences and services quickly. While incorporating software development as an integral part of business may seem like a daunting task, the first important step is to recognize the fundamentally different nature of software's role in business today. This isn't simply a matter of traditional IT with some added responsibility. The ability to deliver customer-facing, software-based experiences is an entirely new capability that you may need to build from the ground up. But you cannot ignore security. Rather, you have to strike the balance between strong security and a great user experience.

In this excerpt from "Digitally Remastered," you'll learn the importance of creating that balance between a good experience and a secure application.

The Security Imperative

Ensuring security across all aspects of the software-driven enterprise has become increasingly complex in the face of rapid technological change. The news is replete with stories about refrigerators sending malicious emails, sophisticated cyber fraud, and cars being hacked while being driven. The challenges will only continue to grow as the number of Internet-connected devices and apps accelerates. It's predicted that there will be 200 billion connected "things" in the world by 20181. All of them will be communicating through software, and all of them will need to be secured to function safely and reliably.

Not that long ago, we just had a few passwords to remember; now we have to think about managing our identity and access across a myriad of cloud-connected apps, services, and mobile devices. The interconnected nature of today's digital ecosystem amplifies the risks. A hacked Twitter account can create immediate reputation damage. And while signing into multiple services with a single social media account is convenient, a compromised account will also compromise every service to which it was linked. Leaked passwords, credit card information, or other personal data can wreak havoc.

The critical role of security in our lives will only increase as the Internet of Things (IoT) introduces new types of vulnerabilities and further raises the stakes. This is because IoT is far more than a set of devices communicating directly with some servers — it is a complex, multilayered mesh that includes sensors, actuators, hubs, data repositories, applications, and messaging frameworks that together make up the IoT ecosystem. Each node in the ecosystem has a unique relationship within it, requiring independent, coordinated interaction without human intervention. Understanding the security implications of all of the relationships within an IoT system is critical to preventing a vulnerability that could turn into the next high-profile security breach on the news.

As the technology footprint of the enterprise expands, so too does the complexity and cost of securing it. At the same time, customer expectations around the safety and security of their digital experiences are increasing. While protecting customer data is the price of getting their business, customers today also demand a seamless, hassle-free experience. They expect you to make security robust and friction-free in a world where the underlying technical challenges are only intensifying. The cost of failure on either side of that challenging balance is extraordinarily high. Not only will users abandon your business if your security keeps them out, 10% percent of them will abandon your brand forever if there's a security breach.

Today, security is much more than passwords and perimeter defenses. It's also about data science, anomaly detection, and predictive analytics — systems and processes that understand your customers' behavior and how your software operates and interacts. Security now also encompasses system self-awareness that can detect and potentially mitigate or stop data breaches, denial-of-service attacks, unauthorized access, and other security failures.

Companies today face cyber attacks hourly or daily; the threats are never-ending and constantly changing. In the digital world, security is not someone else's job. It is everyone's job because security is the primary determinant of trust in a global digital society.

Accountability for security increasingly ends with the Compliance Committee or Chairman of the Board rather than with a Chief Information Security Officer (CISO) because it is so foundational to any business today.

Security is an essential tool for controlling cost, preventing revenue loss, and improving the overall customer experience. For example, banks reportedly want to limit required user interaction to a small proportion of all ecommerce transactions today. Intervening more frequently than that becomes onerous for customers and can result in an increased number of transactions being abandoned with corresponding loss of transaction business. In card payments, for example, analytics allow you to understand a transaction in the context of what is normal for each individual cardholder. Sophisticated modeling techniques are used to assess risk in real-time by analyzing unique authentication data such as device type, geographical location, user behavior, and historical fraud data to separate genuine transactions from suspected fraud. Security analytics technology enables all of this to take place in the background, thus freeing most customers from the inconvenience of having to go through additional authentication steps.

While security technology can create new business efficiencies, the cost of a security failure can be massive. Home Depot's breach resulted in 56 million compromised cards and $63 million in losses; there are 44 civil lawsuits. It cost an additional $60 million to cover reissuing cards and related expenses3. The Target breach had 70 million stolen cards and cost the company $252 million. The CEO resigned, the CIO was replaced, and they hired their first CISO[1].

Identity Is the Perimeter

Digital transformation requires building new digital channels into your business, but doing so eliminates the classic enterprise boundary that had previously provided a degree of protection by having systems shielded from large-scale external access. In the transformed enterprise, the security boundary moves all the way to individuals accessing your company's data on the device of their choice, anywhere, anytime.

This dramatic shift of the enterprise boundary all the way out to the individual user requires rethinking security with the user's identity at the center, and it brings new challenges to consider:

- **Low tolerance for inconvenience**: The explosion of mobility and the resulting expectation for fast, on-the-go access to apps and information has decreased user tolerance for intrusive or complex security processes and resulted in the "consumerization" of technology. Today's customers expect instant access; cumbersome, inconsistent registration and authentication processes can turn them away. Customers desire security with minimal disruption to the task at hand, whether it's checking a bank account balance or checking the status of an order. And the need for convenience isn't limited to consumer applications. Enterprise employees and partners are also demanding easy-to-use solutions to make it easy for them to access corporate information securely and efficiently.

- **Proliferation of privileged accounts**: As businesses digitally transform themselves, access and control of tools and information is spreading throughout the entire organization, outside the control of a single department or centralized function. While broadening the use of technology throughout the business is both a necessary and desirable outcome of transformation, it makes management of privileged accounts more difficult. We've come to think of privileged accounts as those owned by the IT types — network, server, and database administrators — but that is no longer the case. An array of third parties, vendors, and partners may also require privileged access to do their work. The person in marketing who runs your marketing automation tool also has a privileged account. If attackers gained access to his or her credentials, they'd have access to all of your customer data. The same goes for your online sales account management tool, cloud-based storage, and many other examples that may surprise you. More people have non-traditional privileged accounts than you might think, and these types of privileged credentials are involved in the majority of data breaches.

- **Threats are now everywhere**: The rapid expansion of security threats makes it impractical for a single department to protect the entire company. Protecting the company against security threats requires a much broader, multi-faceted approach. Security is a business challenge, not just a technology issue. After all, the cost of a successful external breach is approximately $3.8 million on average, and this does not include the cost of lingering business impact due to reputational damage. Ongoing education both within and outside of the technology organization will help drive understanding and awareness. A regular portfolio review approach focused on security across the entire business will help identify emerging threats, gaps, and mitigation strategies. Given the ever-changing and multiplying threat vectors, detecting vulnerabilities and breaches becomes as important as trying to prevent them. You should assume that malicious actors will find their way in one way or another, and you must be prepared to detect the intrusion and respond quickly to minimize any losses.

Getting Started

Tackling today's security challenges requires broad awareness and participation — everyone must be thinking about the implications of security. The security of "no" based solely on rigid, highly constrained systems is no longer viable. You need to adopt the security of "know" by building insights and dynamic responsiveness into your security strategy. These suggestions can get you started with integrating security as a critical enabler of your business:

- **Build in security as a killer feature.** You need to make security a core principal in all of your software development and deployment from the very beginning. Waiting until the end of the development process to bolt on security is a recipe for creating vulnerabilities and delivering a sub-par user experience. Agile organizations should have security practitioners as part of the delivery team, and security should be an intrinsic part of the planning process. Adopt a "defense-in-depth" approach by securing data and applications at every level of the technology stack. Design and test your applications and services for robust, secure operation while focusing on delivering a friction-free customer experience. You will need to find the right balance between the ideal user experience and the required level of security protection.

- **Make identity your new perimeter**. The enterprise boundary is now the individual user accessing enterprise data via an application or service. Users are the new perimeter in the application economy, and this requires an identity-centric approach to security to ensure that users are who they digitally claim to be. Whether you build your own identity service, federate identity with trusted third-parties, or even enable some logins through social networks such as Facebook or LinkedIn, you must be sure that users are who they say they are and that the information and services they can access exactly matches their role.

  Some data and services may need greater security than others. A user connecting anonymously or with a social login may have some level of access to public data, while other information might require a username and password. Augmenting this basic identity with advanced authentication protocols such as multi-factor authentication (a passcode texted to the user's phone after a login attempt, for example) can help ensure identity authenticity. Risk-based authentication can be used to dynamically adjust ease of use versus risk reduction. For example, a simple password may be sufficient to access balance information in an online banking scenario, but transferring funds may require additional identity verification in order to complete the transaction — an example of "step-up" authentication. Analytics-based security tools can add another layer of validation by combining different sources of data such as location, time of day, transactions, device being used for access, and other seemingly unrelated data to create a probabilistic determination of identity. Using this information, apps could determine whether to automatically allow access, or to request further proof via secret questions or similar unique identifying data.

- **Protect and monitor privileged accounts**. If attackers gain access to a privileged account, they have gained access to sensitive data and/or mission-critical systems and functionality. Insider attacks make heavy use of these accounts as well. You can take these two basic steps to minimize your privileged account exposure:

  - **Grant the minimum amount of access needed for the shortest time possible**. Providing more privilege than required is inviting trouble, and revoking access as soon as it is no longer required — perhaps even on a per-task basis — will keep the window of opportunity for abuse as small as possible.

  - **Monitor privileged access at all times**. Recognize attempts to escalate privileges as well as any behavioral changes from these accounts. If privileged access is compromised, account access histories will help you better understand what happened and why.

Delivering software experiences to your customers requires new pathways into your business that increase the risk of vulnerabilities. There is no longer a clean separation between the inside or outside of the enterprise and security can't be an add-on — it must be integrated throughout the technology stack of your business.

Learn more:

See how CA can help you improve security while delivering a great customer experience.
ca.com/security

Get the entire book:

Download the entire Digitally Remastered book to learn how to fully tool your software factory and drive successful digital transformation.

1 Hiroko Tabuchi, "$10 Million Settlement in Target Data Breach Gets Preliminary Approval," NYTimes.com, March 19, 2015, http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0

CS200-225266-D_1016