PlanFacts

NEWPORT GROUP™

Third Quarter 2018 Issue

Cybersecurity: The Industry's Next Frontier

According to the Identity Theft Resource Center, there were 1,222 data breaches in 2017—exposing more than 172 million records. This easily surpasses the all-time record high set in 2016 of 1,093 data breaches. And that was a whopping 40% increase over 2015's 780 reported breaches.

Cybersecurity fraud was once a problem reserved for the largest government agencies, credit card companies and banks. However, as these organizations have hardened their security capabilities, fraudsters have shifted their focus to the next tier of banks, as well as financial firms that play in the brokerage, retirement and insurance spaces.

Many of these firms are now scrambling to learn from the big banks and quickly implement similar or next generation cybersecurity methods and capabilities.

Defining Cybersecurity

Before you can implement cybersecurity tactics, it's helpful to know what this heavily (and often overly) used term really means.

For the purposes of this article, let's define cybersecurity. It's the art and science of protecting one's data from attacks on confidentiality, integrity and availability. These attacks can come by various means, whether it's social engineering, phishing, unpatched software, social media threats or more advanced persistent threats. But the goals are typically the same: achieving some form of economic or political gain, social justice, or cyberbullying.

Just How Important is Cybersecurity?

As many of us are aware, there is a common behavioral theory in psychology called the Maslow's Hierarchy of Needs. It says that people naturally need to satisfy their need for safety and security first before they can move onward and upward to the next level/tier of need.

I tend to believe there's a comparable hierarchy that exists in the digital space; I call it the "Digital Hierarchy." And just as with Maslow's hierarchy, it assumes that if people don't believe their personal information is secure within the systems they use or access, then no amount of functionality or experience will effectively drive user behavior, utilization or engagement.

Without trust, adoption will be zero.

The Balancing Act: How Cybersecurity Impacts a Company's Investment in Technology

Companies today need to adjust how they balance cybersecurity with functionality and ease of use when it comes to investing in technology and designing and developing systems.

We all want and expect the systems and applications we rely on to perform and support our needs. We want a robust suite of functionality that's easy and intuitive to use, and keeps our information safe and secure. The trick is building and delivering digital solutions that provide all three in a way that is properly BALANCED.

This means that firms may have to invest more time and money enhancing and maintaining cybersecurity than they have in the past. Unless additional resources are made available to accommodate this work, firms will likely have to shift how they allocate resources. They might have to favor additional cybersecurity efforts over the pace at which desired functionality and enhancements can be delivered.

As cybersecurity becomes a larger part of each project, it will require more focus and a greater portion of a project's resources. Without a balanced approach, this could negatively impact the user experience. That's because additional security measures often add additional steps to traditional digital functions: the login/authentication, purchases/transactions, etc. And typically, one's level of delight or satisfaction with the user experience of a particular system or application decreases as the number of steps increases.

Key Trends: Cybersecurity in 2018

There are a number of mature and emerging trends in the cybersecurity space. Here's a quick summary of the ones many firms are investing in now and/or are exploring for the near future:

- *Improving Authentication (User Login/Access):* Strong passwords, multi-factor authentication, multi-tiered authentication, security questions, captcha, SAML-based single sign-on, security/fraud alerts/monitors, biometrics (voice, fingerprint, facial), timeouts, IP address/geography blocks
- *Improving Network/Data Center Security:* Intrusion detection/intrusion prevention systems (IDS/IPS), hardened perimeter protection, distributed denial of service (DDoS), network forensics and analytics
- *Improving Encryption:* Across the span of digital storage devices (SANs, desktops, laptops, mobile, removable media), encrypting data in-transit, encrypting data at-rest, password hashing
- *Expanded Use of Secure Coding:* Ongoing practice of educating software developers to learn from historical and newly identified vulnerabilities to guard against the accidental introduction of such security vulnerabilities
- *Improving Fraud Prevention:* Business measures, procedures and analytics used to recognize and/or prevent potentially fraudulent activities, incident management systems (IMS) to address/deal with fraudulent activities as they occur, identity theft and credit protection monitoring, industry consortiums to share experiences with fraudulent activities amongst peers
- *Expanded Use of Artificial Intelligence (AI):* Defined as pre-defined sets of complex rules/decision-trees applied to large amounts of data; can be used as a method to identify known patterns of activities/behaviors which can be used to predict or detect fraudulent activities
- *Expanded Use of Machine Learning (ML):* Defined as dynamically generating sets of complex rules/decisions from large amounts of data; can be used as a method to identify new patterns of activities/behaviors to predict or detect fraudulent activities
- *Securing the Internet of Things (IoT):* Defined as a system of interrelated/connected computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers that facilitate the transfer of data over a network without requiring human-to-human or human-to-computer interaction; by its highly connected nature, the IoT injects additional security risk into any system connected into an IoT ecosystem

About the Author

Eric Brickman is Newport Group's Executive Vice President of Global Technology and Digital Innovation (TDI). He oversees all of the company's global technology functions as well as digital strategy, user experience and product/platform development and integration.