Exponent®

THOUGHT LEADERSHIP
PUBLISHED 4Q 2018

Promoting Cybersecurity in the Twenty-First Century

November 28, 2018

Data security breach incidents and costs are at an all-time high and continuing to grow year over year. A 2018 Cost of Data Breach Study sponsored by IBM Security estimated the average global cost of a data breach to be $3.86 million, a 6.4 percent increase from 2017.[1] The study estimated the costs of "mega breaches"—or breaches affecting 1 million to 50 million records—at between $40 million and $350 million. In the past five years, the occurrence of mega breaches has nearly doubled with significant costs tied to technical investigations and recovery, consumer notifications, legal and regulatory activities, and lost business.

In efforts to address this staggering cost curve and bolster consumer protection, legislators are increasingly introducing new requirements for safeguarding and protecting individuals' personally identifiable information (PII). The General Data Protection Regulation (GDPR) took effect in the European Union in May 2018, and the California Consumer Privacy Act, A.B. 375, will take effect in 2020 as a potential precursor to federal legislation in the United States.[2] In light of these regulations and the current threat environment, we recommend that companies proactively undertake methodical cybersecurity risk assessments and implement cybersecurity vulnerability countermeasures and safeguards. Such assessments and safeguards can significantly mitigate financial and brand damage risks associated with these twenty-first century cyberthreats.

Commercial companies face several cybersecurity challenges when it comes to implementing secure processes and secure credentials in the workplace. Historically, employees have been one of the weakest links in a company's security armor. Phishing attacks continue to be successful in causing employees to click links that reveal passwords and introduce malware into a system. Smartcards and other public key infrastructure (PKI) based security tokens can offer significantly stronger security than passwords. This is one reason why the Fast Identity Online (FIDO) Alliance has continued to advocate the use and implementation of PKI/cryptographic tokens for authentication. It is also why large corporations such as Google and Facebook have continued to promote FIDO tokens for secure logon and authentication to systems. Adoption of FIDO has greatly increased in recent years because of the enhanced security and user experience offered. In fact, many new system developers have recognized that user adoption is correlated with both a technology's security and its ease of use. Designers of security architectures need to implement safeguards in a manner that enhances user trust and streamlines proper usage as opposed to adding additional security steps that users perceive as barriers to overcome.

Developers of security tokens are also increasingly seeking to satisfy and surpass the most stringent security standards. Chips are certified at high Common Criteria Evaluation Assurance Level (CC EAL) levels whenever possible to protect against most known software and hardware attacks. Whereas attempts to enhance software security and store secure credentials in software are admirable, significantly stronger security can be achieved by housing these credentials in a secure hardware environment that has been adequately evaluated and certified against specific attacks. These attacks include decapsulation, differential power analysis, and other

[1] 2018 Cost of Data Breach Study. IBM Security. July 2018.
[2] California Consumer Privacy Act of 2018. June 2018.

attacks and tampering efforts that an adversary can execute if he or she gains physical possession of the device or credential (e.g., a smartcard, a FIDO token, or the secure partition of a cell phone).

In addition, technology developers are increasingly ensuring that all products that connect to a network or internet have safeguards to protect against cyberattacks. This includes connected autonomous vehicles and Internet of Things devices. Seemingly harmless devices like smart coffee makers or toaster ovens can actually cause significant damage if under the control of malicious actors. In some recent case studies, adversaries gained unauthorized access to systems and sought to rapidly cycle power to cause shorts and ultimately start fires in electronic devices. Similar risks also exist for medical devices that are accessible from a network, including Bluetooth and Bluetooth Low Energy connected devices. Security safeguards can be an important component in optimizing user safety.

Finally, technology developers are increasingly considering how best to balance cybersecurity requirements against the ongoing drive to innovate. Developers can benefit by making cyber resilience a core part of the innovation process. Often, this process is iterative, where testing and verification occur throughout the design process in a continuous feedback loop. When attention to security is part of the design process, many cyber vulnerabilities can potentially be avoided. As an example, manufacturers of surgically implanted pacemakers should consider how best to guard against malicious hacking attempts and attacks as part of the product design process.

Many companies choose to partner with third-party consultants to build and execute comprehensive cybersecurity strategies. Third parties can rapidly and seamlessly integrate into a client's in-house team at a cost benefit that is significantly higher than investment in internal cybersecurity resources. Exponent's multidisciplinary team of scientists and engineers are backed by fifty years of failure analysis experience and are experts in identifying the assets, vulnerabilities, and threats to a product or system. Whether a client is seeking to mitigate cybersecurity threats to a medical device, an industrial control system, or a smartphone, Exponent can offer the depth and breadth of technical expertise needed to get the job done.

Brad A. McGoran, P.E., CSCIP, CSCIP/G, GIAC, ACE-M
Statistical & Data Sciences
Principal Engineer
Menlo Park
(650) 688-7013 | mcgoran@exponent.com

Exponent Office Locations
Atlanta, Austin, Boston Area (Maynard, Natick), Chicago Area (Downtown Chicago, Warrenville), Denver, Detroit, Houston, Miami, New York, Philadelphia, Phoenix, Northern California Area (Menlo Park, Oakland, Sacramento), Seattle, Southern California Area (Los Angeles, Orange County, Pasadena), Washington DC Area (District of Columbia, Maryland, Virginia)

International Offices:
Basel, Switzerland; Derby, Harrogate and London, UK; Düsseldorf, Germany; Shanghai and Hong Kong, China

www.exponent.com