A NEW SECURITY REALITY:
THE SECURE BREACH
Breach Prevention: The Root Cause of the Data Breach Epidemic

According to the 2012 Verizon Data Breach Investigations Report, there were 855 data breach incidents reported in 2011 involving 174 million records – the second-worst year ever.¹ According to Forrester Research, security spending in 2007 represented 8.2% of total IT spending. In just three years, it had risen to more than 14%.²

These statistics summarize today’s reality in IT security: security is consuming an ever-larger share of total IT spending, but security effectiveness against the data-breach epidemic is not improving at all. The root cause of this trend is captured in the spirit of Jack Welch’s quote: enterprises are not investing in security based on reality as it is; they’re investing based on reality as it was: a bygone era where hackers were glory-seeking vandals, sensitive data was centralized, and the edge of the enterprise was a desktop PC in a known location. In this reality, network firewalls and other network perimeter “breach-prevention” technologies were good enough.

Unfortunately, yesterday’s “good enough” approach to security is obsolete in an age where data is distributed across and beyond the enterprise, the edge is diffuse, hackers are skilled criminals, and insiders – both malicious and otherwise – are a constant threat to data compromise.

There is nothing wrong with network perimeter security technologies – they do what they were designed to do for the glory-seeking vandal era. The problem is, many enterprises today rely on them as the foundation of their data security strategy: breach prevention. Importantly, market trends show they have no plans of changing this approach. According to IDC, of the $28.4 billion enterprises spent on security technology in 2011, more than 26% ($7.4 billion) was invested in network perimeter security products – the poster-children of the breach-prevention strategy. In addition, IDC projects that this breach-prevention market will grow at a healthy 6.4% annual rate through 2016.³

If IDC’s projections are accurate and breach-prevention technology continues to consume a growing and disproportionate amount of enterprise-security investment, the enterprise data-breach epidemic will be as vibrant as ever in 2016. In fact, it will likely be much worse than it is today, because while enterprises invest in reality as it was, adversaries are thriving and innovating in reality as it is.

¹http://www.verizonbusiness.com/about/events/2012dbir/
From Breach Prevention to Breach Acceptance

The Verizon report indicates that employees and other insiders perpetrate more than 50% of all intellectual property thefts. So by definition, breach prevention is an irrelevant strategy for data protection because every organization already has potential adversaries inside the perimeter. In this environment, the core of security strategy needs to shift from “breach prevention” to “breach acceptance.” And, when one approaches security from a breach-acceptance viewpoint, the world becomes a relatively simple place: securing data is the top priority, since the lust for data is the only reason why you are being breached in the first place.

Obviously, securing data is a challenging proposition in a world where cloud, virtualization and mobile devices are causing an exponential increase in the attack surface. Many organizations are applying the age-old concept of “containment” to this problem: limit the places where data can go, and only allow a limited number of people to access it. However, this strategy of “no” – where security is based on restricting data access and movement – runs counter to everything technology enables today. The mandate today is to achieve a strategy of “yes,” which is built around the understanding that the movement and sharing of data is fundamental to business success. If we look out to 2020, the winner of “Chief Information Security Officer of the Decade” will not be a CISO who said “no” to cloud, virtualization and mobile. It will be a CISO who said “yes” to these trends, and did it in a way where data remained secure.

Introspection

Resolve that the current approach to security is not working as it should, and that it is time to try something new.

Acceptance

Face reality as it is: breaches are inevitable. Once one accepts this reality, it becomes possible to formulate a strategy for more effective data protection and a more solid overall security posture.

Understanding

Know your adversaries – both internal and external – and understand that they want an acceptable return on investment (ROI) just like any business. Once you've done this, you can build a Secure Breach security strategy designed to impair adversary ROI.

Action

Implement the technology and controls required to mitigate human error and decrease adversary ROI. Car thieves will always start with unlocked cars – data thieves are no different. If it's too difficult to steal data, they'll simply move on.
From Breach Acceptance to the Secure Breach

It’s one thing to change one’s mindset. It’s another to implement a new approach to security. While there is no “one size fits all” prescription for achieving the Secure Breach reality, there are two primary areas of focus:

Area 1: Moving controls closer to the data.
Adversaries are after your data. Therefore, you should move your security controls as close as possible to the data. This means identifying assets that have a strong potential adversary ROI, and then making it much more difficult to achieve that ROI by coupling strong identity and access management (IAM) with data encryption. If you are who you say you are, you can access the data. If you’re not, the data you access will be unusable.

This is not an entirely new concept – the promise of data encryption is familiar territory for most security professionals. However, the technological capability to encrypt data on an enterprise scale, in a centralized way that does not disrupt the flow of business, is relatively new. Modern encryption technology (crypto) has largely overcome the performance and complexity issues of the past. However, it still needs to be implemented correctly – because crypto done wrong is worse than no crypto at all: it can give a false sense of security (thinking you’ve encrypted all your sensitive data when you haven’t), or it can disrupt your business (if you can’t manage the keys in a way where data is available when you need it.)

There are three key steps to deploying crypto in a way that enables a true Secure Breach environment on an enterprise scale:

• First, build a crypto foundation providing a trust anchor for the implementation of encryption enterprise wide. This foundation handles important tasks including secure key generation, storage, archiving and termination.

• Next, implement enterprise key management to create and enforce policies during the life of a key and its use, and to ensure the keys are available to the information and applications across the enterprise.

• Finally there are the encryption enforcement points themselves that leverage the enterprise key management and crypto foundation, including native encryption functionality in applications as well as third-party encryption solutions. These encryption enforcement points already include applications, databases, files, storage, backup, servers, virtual machines, and communication methods, in locations ranging from traditional infrastructure to public clouds.

One of the most essential areas enabling enterprise-scale crypto is advancement in encryption key management. The volume and variety of data that needs to be encrypted in a Secure Breach environment means potentially millions of encryption keys supporting the vast infrastructure and applications of a global enterprise.
When each of these components has isolated, disconnected key management, it becomes nearly impossible for an organization to adequately protect the encryption keys. And if keys are compromised, so is the data, and there is no longer a Secure Breach environment. If keys are deleted, even inadvertently, the encrypted data is effectively deleted too.

Modern key-management solutions enable centralized management of the entire key lifecycle across the extended enterprise. This ability to have centralized key management provides the ability to disintermediate individual applications of encryption from the critical processes of protecting keys, delivering federated encryption capabilities with a reliable trusted key lifecycle.

At the macro level, this approach to crypto finally provides the scalable framework required to attach security controls to the information itself – a prerequisite for enabling a Secure Breach environment. When one can apply controls at this level, one is much less dependent on perimeter or infrastructure-level controls for data protection. This is critical when looking at how to leverage the operational benefits and cost savings of new IT trends like consumerization, virtualization and cloud, all of which significantly change the span of control.

Attaching security directly to the data also enables organizations to confidently operate without requiring complete control of the entire computing stack, from hardware through data. When data is encrypted, administrators of infrastructure no longer have access to the sensitive or protected information. They can continue to administer and operate systems, performing critical functions to ensure functionality and availability, but cannot access any of the data because they do not have the encryption keys.

©2013 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.
Area 2: Improving the ability to detect and respond to breaches.

Most modern security attacks start with a very fast but undetected breach, followed by an extended period of time where the intruder silently siphons off data. According to the Verizon report, it takes months or years for enterprises to detect a breach and 92% of the time they don't even detect it themselves – instead they are told about it by a customer, partner or some other third party.

While data encryption makes it much more difficult for adversaries to steal anything of value, it is still important to detect and remove them as quickly as possible. This requires an evolved situational awareness strategy that facilitates the anticipation, discovery and investigation of anomalous behavior. In fact, this is an area where firewalls and other network perimeter defenses can provide a great deal of value – as sources of data contributing to total situational awareness.

There are many tools available today that can help with situational awareness (security information event management systems, IAM, anomaly detection, etc.). However, beyond technology, a situational awareness program should include “human intelligence” considerations like:

• Understanding adversaries and emerging threats.
• Understanding normal business activity both within and beyond the enterprise, and how it maps to the underlying technology infrastructure.
• Understanding the identities and roles of people, machines and software.

By marrying technology and business context, enterprises can more readily identify anomalous behavior and shorten the timeline between initial breach and threat remediation.
The Secure Breach Future

The current mass-market perception of data breaches is relatively naïve. Breaches continue to be positioned as sensational events in the headlines, and rarely is there an understanding of today’s reality: not all breaches are the same. In fact, not all breaches are “bad” breaches either.

For example, Zappos and Lockheed Martin received significant negative media attention for their breaches. A few outlets, however, were savvy enough to write positive stories about them, because both had taken sound security precautions to meet regulatory requirements and protect sensitive assets. According to publicly available information, these breaches were, for the most part, Secure Breaches – intruders penetrated the network perimeter, but they were unable to access valuable data.

As enterprises move into “reality as it is,” the ripple effect will be that mass media and the population at large will evolve its perceptions of data breaches. They too will move from a “breach prevention” mindset, to one of breach acceptance. The fact that a breach has occurred will no longer be the “news.” Rather, news value will be determined by the answer to this question: “Was it a Secure Breach?” Breaches will become like the weather – major hurricanes will garner headlines; drizzly days will not.

All current trend-lines lead to more data breaches. Enterprises are investing significant security dollars to extend the life of the obsolete breach prevention strategy, adversaries are continuing to innovate and thrive, and the extension of the enterprise into the cloud and onto mobile devices is greatly increasing the potential attack surface and the likelihood of accidental data exposure or loss.

These trends all point to a consistent theme – security needs to be attached to the data, so enterprises can maintain control of the data even when it is deployed in the cloud or on mobile devices, and even when it falls into the hands of adversaries. Trying to keep today’s adversaries out of the enterprise through breach prevention is a fool’s errand (even adversaries that are not terribly sophisticated). However, using crypto on an enterprise scale to reduce the value of data to near zero for unauthorized users is not only possible; it is being done today, as the Zappos and Lockheed examples show us. It is also a requirement for transitioning from a strategy optimized for “reality as it was” – breach prevention – to a strategy optimized for “reality as it is” – the Secure Breach strategy.