VERA

BUILDING A DEFENSIBLE SECURITY PROGRAM

Align teams, address systemic risk and maintain stakeholder trust

TABLE OF CONTENTS

Introduction

For several years now, we've seen an increase in the number of chief executives either resigning or being fired after their company suffered a data breach. In fact, research shows that twice as many CEOs are being fired over cybersecurity incidents than are CIOs or CISOs. It's happening so often, the public is becoming numb to news like this -- it's even expected.

According to Gartner, by 2022, 50% of CEOs who lack cybersecurity postures that are defensible to their key stakeholders will be fired following material breach incidents that impact greater than 25% of their customer base.

CONSIDER THE STATISTICS...

1. In March of 2017, both the CEO and Lead Attorney for Yahoo! were fired.
2. In September of 2017, the CEO, CIO and CSO of Equifax stepped down.
3. In November of 2017, both the CEO of Uber resigned, while their Chief Security Officer was fired, after their 2016 data breach.
4. The CSO and CISO of JPMorgan Chase reassigned following their data breach in November of 2015.
5. Following Home Depot's data breach in 2016, the CEO resigned.
6. The CIO and CEO of Target both resigned following their massive data breach in 2014.

But let's step back for a moment. In today's world, after such huge upticks in data breaches, executives don't need a wake-up call, nor do they need more advice about security budgets. In most cases (exceptions noted), organizations actually have adequate security budgets and spend accordingly on great solutions.

Is your organization doing enough to protect its data and can you defend your choices in the event of an incident?"

Where's the Disconnect?

What we've observed in the industry is that it always comes down to one thing -- the systemic and cultural issues that can often stand between IT and non-IT employees, trying to create the right level of security that allows for strong protection and the need to stay productive to achieve business outcomes.

In addition, it's not necessarily a problem with the chosen security stack, but the lack of defensibility of the program that was put into place. To clarify, we don't mean defense against "hackers", but the ability or inability to defend the security investments with customers, board members, and shareholders. This is exactly why more non-IT executives are being held accountable in the event of a data breach.

"The industry average for finding malware is approximately 90 days, and our security team caught it in 30 days."

The Ultimate Goal: Defensible Security

What is "Defensible Security"? The most simple explanation of defensible audit is a security program that can answer the question from stakeholders, "Is the organization doing enough to protect its data and information resources and can we defend our choices in the event of an incident?"

Some examples of defensible security:

"The industry average for finding malware is approximately 90 days, and our security team caught it in 30 days."

"We patch within X amount of hours except in situations where business reasons exist to accept risk. Here is a list of exceptions and their patch windows."

"The application patch was delayed by six business days for customer service reasons. This is reasonable within industry best practices."

Lessons from an Epic Fail

Equifax is perhaps one of the best examples of an indefensible situation. In 2017, Equifax was breached due to a third-party library vulnerability in their code -- Apache Struts. (Apache Struts is an open source MVC framework for Java). Apache Struts helps developers build complex applications by reusing components for certain tasks. The Apache Struts patch was available in March of 2017, but Equifax failed to remediate, and was notified of the breach in September of that year.

Why would anyone, especially in a large organization that deals with the data of hundreds of millions of consumer data, leave a critical vulnerability unpatched for months? That's a long and complex answer, mostly having to do with budget, risk, and accountability inside the organization that let it happen.

In December 2018, the House Oversight Committee released a final report that states, "Equifax should have addressed at least two points of failure to mitigate, or even prevent, this data breach. First, a lack of accountability and no clear lines of authority in Equifax's IT management structure existed, leading to an execution gap between IT policy development and operation. This also restricted the company's implementation of other security initiatives in a comprehensive and timely manner. As an example, Equifax had allowed over 300 security certificates to expire, including 79 certificates for monitoring business critical domains. Second, Equifax's aggressive growth strategy and accumulation of data resulted in a complex IT environment. Equifax ran a number of its most critical IT applications on custom built legacy systems. Both the complexity and antiquated nature of Equifax's IT systems made IT security especially challenging. Equifax recognized the inherent security risks of operating legacy IT systems because Equifax had begun a legacy infrastructure modernization effort. This effort, however, came too late to prevent the breach."

Top executives, including the CEO, the CIO and the Chief Security Officer all resigned, as these issues and lack of action taken, were not defensible.

Can it be done?

For a program to be truly defensible, there are both technology and business best practices that must be followed to ensure success.

TECHNOLOGY BEST PRACTICES: DYNAMIC DATA PROTECTION

1

Encrypt all non-public information that is stored or shared inside or outside the company: It's important to apply encryption to sensitive files at rest, but also anywhere your data is transmitted -- whether that's through email, Box, Dropbox, Sharepoint, or other collaboration tools. VERA encrypts your data with strong AES-256 bit encryption and goes further to prevent unwanted viewers to your information anywhere that information moves and applies data-in-use protections that control and limit what recipients can/cannot do with your firm's nonpublic data.

2

Encrypt all non-public information that is stored or shared inside or outside the company: It's important to apply encryption to sensitive files at rest, but also anywhere your data is transmitted -- whether that's through email, Box, Dropbox, Sharepoint, or other collaboration tools. VERA encrypts your data with strong AES-256 bit encryption and goes further to prevent unwanted viewers to your information anywhere that information moves and applies data-in-use protections that control and limit what recipients can/cannot do with your firm's nonpublic data.

3

Implement an Audit Trail to Reconstruct Transactions and Log Access Privileges: In the past, requirements for an audit trail on data access was seen as an add-on or even an afterthought. Now, some regulatory mandates call for improved visibility into data use, which highlights the need for an automated way to track and log access privileges and reconstruct transactions. VERA provides granular 360-degree visibility into all access attempts of your nonpublic information (both authorized and unauthorized attempts) with a full audit trail of who, where, and how your firm's data was accessed to help you build a better picture of your data use. You can also export VERA's audit log into your favorite SIEM/BI tools for further monitoring and detailed analysis.

4

Real-Time Access Control: Simple encryption and common security tools like Data Loss Prevention (DLP) are great technologies, but they cannot remotely destroy nonpublic information once it's sent beyond the organization. VERA gives you control of your data through its entire life cycle, as it moves beyond your systems, through the proverbial "last mile" to another partner's desktop, phone, or cloud application. It offers flexible, customizable policies, including the ability to 1) automatically expire information after a defined period (time-bomb); 2) easily create rules that provide for data retention; and 3) revoke access to any user, at any time, at the click of a button.

Business Best Practices: Expanding Beyond Security Teams

One of the biggest lessons the industry has learned is that decisions about security investments can't be made in isolation by the security team. We all understand that security is a business issue, so why do many organizations still hold security departments as the only one responsible and accountable for security programs? Companies would benefit from expanding decision-making to include other departments such as legal, human resources, and privacy officers to make sure leaders in all areas of the business are aware of the risks to their department as well as the entire company.

Alignment with Proven Practices and Standards

Another aspect of defensible security is the ability to prove that the organization is in alignment with industry practices and standards. This means using reference models such as NIST cybersecurity framework, ISO/IEC 27001/2 or CIS Critical Security Controls, to guide decisions. It's also recommended that organizations create an Information Security Charter. This is usually a short document that establishes accountability for protecting all sensitive information, and provides directives for executives, namely the CISO, to build and manage the program.

Privacy by Design and Security by Design

With the stakes raised, the pressure is on Privacy leaders and Data Protection Officers to ensure their organizations are correctly managing sensitive data. Yet they are generally expected to do it on shoestring budgets and limited resources. Recent research from CPO Magazine reveals that 46% of their 250+ survey respondents allocate less than 5% of their annual governance, risk and compliance budget to data protection and privacy; another 20% allocate between just 5 to 10%. With security budgets continually increasing, privacy efforts are usually left with very little funding. In that constrained environment, what should privacy officers focus on?

Educating and engaging senior leadership: Privacy needs to start from the top down. Senior executives have woken up to the significant consequences data breaches can impose - financial loss, regulatory action, shareholder suits, and even some executive job losses (think Equifax, Sony, Yahoo, and many more). While data security is now top of executives' minds, leaders, especially in unregulated sectors, must understand that privacy, while tangential, is a separate issue. Senior leaderships' example of a strong privacy ethos and practice is an absolute must for an organization to follow. An organization's privacy team has a major role to play in guiding and advancing that posture. And that leads to... Driving a privacy-aware culture. Senior leaders and privacy teams need to help all staff understand, accept and implement effective privacy measures. It's challenging to change organizational behaviors across especially when everyone is moving at warp speed. Training programs, awareness-raising campaigns, executive messaging and consistently integrating privacy into normal course-of-business discussions will move the needle. Laws and regulations are changing all the time, so the privacy team needs to stay on top of what's new and continually guide the organization.

Data governance. Controlling access to sensitive data goes a long way in protecting it. Privacy and Security teams need to partner to drive a governance framework that accounts for the access, tools, skills and change management needed to make privacy work in their organization. That framework must account for proper data stewardship, including managing permissions, appropriate use, and data quality. The fewer hands touching any given data set, the lower the risk.

Driving execution of data mapping and clean-up. Governing data requires that you know what you have and where it is. With cloud-centric environments and extensive 3rd party data exchanges, this is especially challenging. Privacy teams own the very heavy lift of directing every organizational department that uses sensitive customer and employee data to map what they have and where it goes, to the best of their knowledge; if a data audit reveals problems, a clean-up effort is required. You can imagine the significant resistance to such an involved exercise! Senior executive support is crucial to driving this step.

Guide privacy-by-design (PBD). Retrofitting existing systems for privacy is difficult. As new systems are planned and developed, it's best to integrate PBD so that privacy-centric attributes are integrated from the beginning. While this is normally associated with new IT development, PBD can be baked into any process that involves gathering and/or using sensitive data. Privacy teams set PBD guidelines that are shared throughout business units for use as they stand up new systems and processes.

Customer Case Study: Pokémon and Defensible Audit

Pokémon GO exploded in popularity when it was first launched in 2016 and continues to enjoy high activity levels. Two years after its launch it saw 5 million daily active users, with over 800 million downloads. The overnight success of the augmented reality game put the small information security team at Pokémon under pressure, with an influx of users' personal identifiable information (PII).

In addition to securing end-user PII, the Pokémon information security team is responsible for protecting intellectual property relating to its animated TV series, movies, home entertainment, and website. To successfully launch and promote new products, the business relies on sharing sensitive intellectual property among employees and external stakeholders. They needed a secure way to share rich media files, game designs, and new character ideas, allowing for mass collaboration and dynamic editing over a lengthy production process.

With increasingly complex security requirements, the IT team wished to bake security into business operations in an automated fashion. They adopted VERA to enable seamless collaboration and

USE CASE 1:

Protect Personal Identifiable Information (PII)

Pokémon GO and other games generate a great deal of sensitive user data, including name and locations. With increasingly strict state, federal and international data protection regulations, the Pokémon information security team needed an auditable way to control access to data as it moved across internal systems.

Pokémon deployed VERA to encrypt files which contained PII and track these files wherever they traveled. Each file is encrypted with a unique key that is secured within the VERA Platform. Security policies define which personnel can access these files, and the actions they can perform with this information.

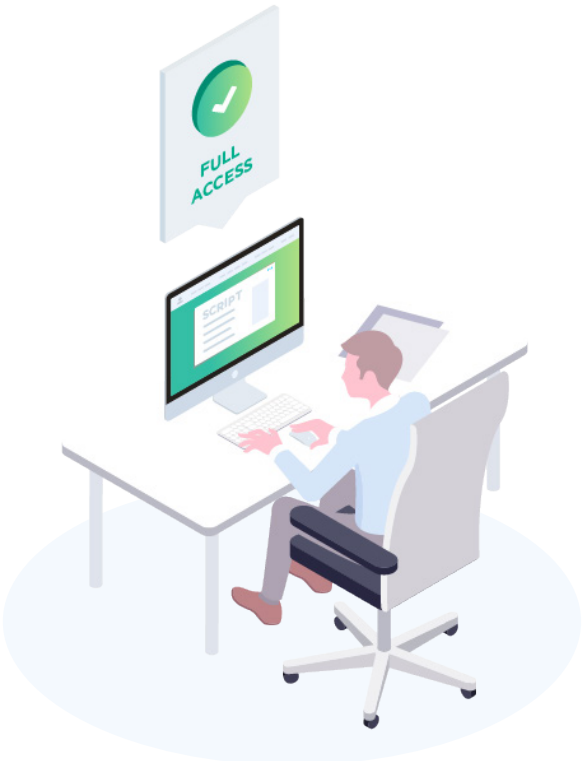
For authorized users, encryption and decryption happen behind the scenes, with no need to download agents or install plugins to access data. VERA's technology protects against man-in-the-middle attacks, preventing unauthorized access to PII from malicious actors.

Audit logs are available through the VERA Dashboard, showing all successful and unsuccessful attempts to access information. This creates a chain of custody, allowing the information security team to demonstrate compliance to regulations and ensure control of all PII.

USE CASE 2:

Secure Sharing of Intellectual Property

Pokémon employees use cloud collaboration platforms such as SharePoint and DropBox to move information between organizational teams and third parties. The security team was confident of controlling information within their own environment but recognized the risk of sensitive files landing in the wrong hands after leaving their network. Rather than restrict information sharing, which employees relied on to perform their jobs, the security team needed a way to retain control of intellectual property stored in cloud platforms or downloaded onto external devices.



With VERA, they could secure at the document level using encryption capabilities that followed data outside the Pokémon environment. Designers could send new artwork to third parties, while retaining control over user access and which actions were permitted, such as forwarding or copying.

Pokémon leveraged integrations with popular cloud sharing applications for swift and simple deployment. By automating the encryption of files shared externally through DropBox and other applications, they avoided issues with user adoption, securing enterprise data no matter which application or device it resides on.

Dynamic file protection makes sure that file content is always secure, even while in use. This is done by using VERA's patented Always-on File Security and capturing all calls between the application layer and the system layer. Granular visibility and centralized control are other capabilities so the Company understands how their content is used, by whom, and can proactively investigate unauthorized access attempts. In addition, policies can be based on a number of pre-defined parameters including file location, name, type, securer, sender, recipient, group, or other pre-existing permission structures.

Summary

VERA's dynamic data protection platform is the intelligent, seamless and proactive solution that many firms leverage to secure all corporate data through its entire life cycle. This protection cannot be stripped off the file the moment it's downloaded or opened by a recipient. Your team is empowered to always enforce your company's security control and usage policies on highly sensitive files, even after data is shared outside of your team, downloaded, duplicated or moved to unmanaged domains.

In the event of a breach, whether from an outside actor, intentional misuse, negligence, or just smart people making an honest mistake, VERA gives you the tools to update or revoke access, instantly, to all copies of the file or specific users or vendors.

With VERA, you can control:

WHO:
Who has access to your files unauthorized) access attempts with a full audit trail. Anywhere your files travel

WHAT:
What they can/cannot do with them (e.g., edit, view only, block copy/paste, add watermark) with a full audit trail. Anywhere your files trave

FOR HOW LONG:
For how long collaborators can access (e.g., automatic time expiration, retention rules, granular revoke access capabilities)

AUDIT:
Audit all authorized (and unauthorized) access attempts with a full audit trail. Anywhere your files travel

VERA

BUILDING A DEFENSIBLE SECURITY PROGRAM

HIPAA

Any healthcare, pharma, or medical company that deals with patient data

For the healthcare industry, patient confidentiality is paramount. The average cost of a breach in the US related to patient data is over $10M dollars, with fines attributed to each instance data breached - not just a singular file, etc.

HOW VERA HELPS

- VERA logs every action taken by any user on a VERA-protected file.
- VERA logs every administrative or system action within the VERA system.
- VERA's detailed audit logs provide defensible proof against data breaches.
- Ability to provide proof of breach reduces the overall requirement by the customer to report a breach occurred.
- Audit log reduces overall financial and brand implications associated with a breach.

NYDFS Part 500

Cybersecurity Regulation for Financial Services in NY State

Encrypt all "nonpublic information held or transmitted" in the firm. Restrict access privileges not only to systems but to the data itself. Implement an audit trail system to reconstruct transaction and log access privileges. Provide for the retention and "timely destruction" of nonpublic information.

HOW VERA HELPS

- VERA leverages military-grade en cryption for protecting customers' sensitive file data.
- VERA's dynamic access control en sures only the right people/parties have access to the data.
- VERA's detailed audit logs provide defensible proof against data breaches.
- Ability to provide proof of breach reduces the overall requirement by the customer to report a breach occurred.
- Audit log reduces overall financial and brand implications associated with a breach.

PCI Compliance

Any company that is collecting and storing customer credit card data

For the healthcare industry, patient confidentiality is paramount. The average cost of a breach in the US related to patient data is over $10M dollars, with fines attributed to each instance data breached - not just a singular file, etc.

HOW VERA HELPS

- VERA logs every action taken by any user on a VERA-protected file.
- VERA logs every administrative or system action within the VERA system.
- VERA's detailed audit logs provide defensible proof against data breaches.
- Ability to provide proof of breach reduces the overall requirement by the customer to report a breach occurred.
- Audit log reduces overall financial and brand implications associated with a breach.

VERA

GENERAL DATA PROTECTION REGULATION

Any enterprise that operates or does business affecting European Citizens

Right to be forgotten. On request, all personal data must be destroyed.

HOW VERA HELPS

Eliminating particular files simply by making them inaccessible individuals can be encrypted with a singular key- at which time a user requests their data to be "forgotten" revoking access or deleting the key for this user would render that data useless - even data that is out of the companies physical control

HOW VERA HELPS

VERA leverages military-grade encryption for protecting customers' sensitive file data. Automated protection enforced for employees, partners operate securely and our customers have control of their data. VERA's dynamic access control ensures only the right people/parties have access to the data. Granular document policies enforce data in use protections restricting 3rd party processors from exfiltrating sensitive personal information VERA logs. every action taken by any user on a VERA file

Data protection by design, and by default, ongoing protections and tracking.

Data controllers can only use sub-processors with adequate security; enforcing protection while working with 3rd parties.

HOW VERA HELPS

VERA's dynamic access control ensures only the right people/parties have access to the data. Granular document policies enforce data in use protections restricting 3rd party processors from exfiltrating sensitive data. VERA logs every action taken by any user on a VERA-protected file

HOW VERA HELPS

logs every action taken by any user on a VERA-protected file. VERA logs every administrative or system action within the VERA system

Maintain records of processing activities, who had and has access to data.

Security of processing.

HOW VERA HELPS

Data encryption. Dynamic control of access and usage of data. Detailed audit and tracking to ensure data integrity

HOW VERA HELPS

VERA's detailed audit logs provide defensible proof against data breaches. Ability to provide proof of breach reduces the overall requirement by the customer to report a breach occurred. Audit log reduce overall financial and brand implications associated with a breach

Notification of a personal data breach to the supervisory authority. 72-hour breach notification. Any data encrypted is not required to be disclosed.

Notification of a personal data breach to the supervisory authority. 72-hour breach notification. Any data encrypted is not required to be disclosed.

HOW VERA HELPS

VERA's detailed audit logs provide defensible proof against data breaches. Ability to provide proof of breach reduces the overall requirement by the customer to report a breach occurred. Audit log reduce overall financial and brand implications associated with a breach

HOW VERA HELPS

VERA protection leverages military grade encryption VERA provides both manual and automated file protection based on a cloud-based rule/configuration engine. Dynamic real-time access control and granular data in use protection within native applications

Personal data must be protected and used for only specific purposes.

"Special categories" of personal data must carry extra protection.

HOW VERA HELPS

VERA protection leverages military grade encryption VERA provides both manual and automated file protection based on a cloud-based rule/configuration engine. Dynamic real-time access control and granular data in use protection within native applications