FORTRA

WHITE PAPER (Titus)

How a Culture of Security Drives Brand Trust

Brand Trust and Security Culture in Today's Workplace

Trust in an organization influences the decision making of customers, partners and investors. Building brand trust takes time and effort, but it can unfortunately be lost in an instant. Data breaches are not only financially costly, they can be devastating to the trust an organization has built up in the market, and can lead to long term losses. Digital transformation allows employees greater means to collaborate, but also increase the potential for data leaks; in a well-meaning effort to share information and increase productivity, employees may unintentionally leak data. Creating a culture of security is a vital step in preventing breaches, and thus in protecting brand trust.

The Relationship Between Data and Trust

As per CIO Insight, "In an increasingly complex and connected world, the ability of an organization to collect, manage and analyze data effectively separates the winners from the runners-up." In the world of Big Data, information is the new currency of business; it flows into and through organizations, out into the cloud, and across the Internet of Things.

There are market expectations and regulations stipulating that all sensitive data within an organization's custody be strictly protected. All organizations must therefore act as true data custodians, treating sensitive information responsibly and appropriately to ensure that it is not breached. It is no longer only intellectual property that must be protected, but highly sensitive personal information, including Personally Identifiable Information(PII), Payment Card Information (PCI), and Protected Health Information (PHI).

Because Big Data is driving business outcomes, it is more important than ever to maintain trust – if trust is lost, not only is the brand damaged, but employee access to data will be severely diminished if not entirely cut-off.

Defining a Culture of Security

Many of the advancements in a digital workplace are built to help people do their jobs better, offering greater and easier access to information as well as modern collaboration tools and techniques. But the more data travels, the more it's at risk of being breached. While organizations invest heavily in security end points, the employees themselves are often overlooked or ignored. Given how much sensitive information users create, consume, share, and store, overlooking employees creates a major gap in any security strategy.

There is no question that investment in security technology is vital in the fight to protect an organization's valuable data assets. Making your users part of the solution unlocks a huge opportunity. This doesn't mean relying on them entirely, nor negatively impacting their workflow – it means educating and empowering users to make better decisions on how information is handled.

According to Forrester, 56% of user driven breaches are unintentional. As such, fostering user education and empowerment can significantly strengthen security. A well-intentioned user who is aware that the document they are sending contains client PII can apply educated caution when selecting email recipients. Additionally, warning a user when they are about to break a security policy will not only prevent that incident, but also serves to educate them, and increases their awareness regarding how sensitive information should be treated in the future.

The Impact of Digital Transformation

Digital transformation itself is described in thousands of articles, papers, and research notes, all available online, and the purpose of this discussion is not to directly explain it. One recurring theme that leads to security challenges, though, relates to the fact that IT no longer has full control over the tools and technologies being used across the enterprise, nor the way in which they're being implemented.

The speed at which data can be collected, shared, consumed, and analyzed has a massive influence on its value, but with speed comes risk. This is manifested in not only the pace at which employees are sharing data, but also in the rate at which new technologies are implemented across the organization.

Many technologies are often selected and at the business unit level, or sometimes even by a few individuals, and the primary focus is thus usability rather than security. Without a culture of security built into the organization, employees are more likely to put efficiency ahead of data protection, increasing the risk of a chain reaction of breach and loss of trust.

While a culture of security doesn't replace intelligent security investments, implementing one without the other severely restricts an organization's ability reach the full business potential of a digitally transformed business.

Alignment of People, Process, and Policy

The ideal security solution addresses people, process and policy; people relating to the culture of security, process relating to the way they do business, and policy relating to the given security rules within the organization. If an organization creates a culture of security and enforces security policies, but forces people through a workflow that is unnatural or cumbersome as a result, people will simply find a way around it. For security solutions to succeed, they must empower users to act appropriately within their workflow, and enforce policies when users or processes violate security rules.

A methodology of *Educate, Empower*, and *Enforce* brings people, processes and policy together, while ongoing *Monitoring* allows for optimized control and agility.

- **Educate:** Periodically training users on security policies isn't sufficient. Effective education requires continuous, on-the-job education as employees are going about their daily work routine. And education does not stop at end users - organizations can "educate" security applications and solutions to allow for scenario-appropriate action to be taken based on the sensitivity of a file rather than a broad-brush approach. Visual markings and alerts, for example, notify a user know about the type or sensitivity of information or data, while complementary file metadata allows a data loss prevention (DLP) tool to apply appropriate action given the information's sensitivity. This enables linking business decisions to data value and risk.

- **Empower:** Employees are expected to abide by the governing security rules and appropriately protect information, but are usually not provided real measures by which to do so. As a further step to education, empowerment means truly enabling security ownership, rather than just expecting it, to strengthen information governance. Users are also empowered to make proper use of digital workplace technologies, enabling secure collaboration.

- **Enforce:** Even with education and empowerment in place, mistakes and violations may still occur. A level of enforcement is required to act as a safety net. This enforcement ensures that data protection policies are applied, preventing the user from mishandling sensitive information.

- **Monitor:** Monitoring users' behavior with sensitive information is essential for improving data protection. Effective data monitoring requires accurate identification of sensitive data, how it is being shared, when it is being put at risk, and which users represent an insider threat. This allows organizations to spot risks and take action. Even if inappropriate action was prevented (e.g. sensitive email was blocked from being sent outside the organization),

it may indicate the need to retrain certain individuals or update security policies. A successful monitoring program allows an organization to measure the success of their security solutions and to ensure that their valuable data assets are sufficiently protected.

How Titus Can Help

With over a decade of experience helping organizations transform their security culture and protect their data, Titus understands the critical success factors of navigating the current digital business transformation.

Data classification empowers both people and security technology to make better information governance and sharing decisions. Titus is uniquely positioned within your organization, at the intersections where information is created, accessed, processed, protected and shared.

Titus engages users within their daily workflow by educating and empowering them to become a part of the security ecosystem. As your users become more security conscious, they will make better decisions when handling sensitive information and avoid engaging in any activity that could put information at risk.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.