Why Relying on Encryption Leaves Consumers Exposed

It has always been important to protect customers' information, but for many businesses, the cost of implementing security has prevented it from being a top priority.

That's going to change.

Consumers, governments, and shareholders are going to require corporations to own up to delivering better solutions to protect customer data.

Security breaches within major companies such as Target, Barclays, and Apple have shoved cybersecurity back into the spotlight. Data protection is now becoming the No. 1 priority for enterprises. However, this mad dash to put in stop-gap fixes has led to panicked and half-formed solutions — placing Band-Aids where there should be full-scale surgery.

When it comes to protecting vital information, the most common solution is encryption. Although it's a critical step, it's only one piece of the bigger cybersecurity puzzle.

Why you should encrypt

While it's only a single component of security, encryption is a requirement for your enterprise.

- **It prevents people from reading your data.** Simply put, properly implemented encryption makes it very difficult for bad actors to read protected consumer data.
- **It's the right thing to do.** Anything you can do to protect your consumers' privacy and data is critical to business. Proper implementation of Secure Sockets Layer (SSL) and other encryption methodologies throughout your enterprise architecture significantly helps protect the financial and private information transmitted and stored across your networks.

• **It can be an obstacle to hackers.** While encryption didn't deflect the Target security breach, in other cases, it has prevented hackers from getting customers' actual PIN numbers. Thanks to strong encryption, customer information has been protected from immediate cracking, allowing customers enough time to change their access codes or order new debit cards.

Why encryption can't solve everything

While encryption is vital when it comes to protecting sensitive information and financial transactions, thinking it will solve everything can be dangerous.

• **Obfuscation and protection are different.** Even if your data is encrypted, the fact remains that it can still fall into the wrong hands. Encryption is the envelope, and your information is the letter. Once an attacker has figured out how to open the envelope, few companies can protect the letter. Intercepting communication and altering it for other purposes can wreak havoc.

• **Major security breaches often don't involve encryption.** Out of the three most prominent security breaches in the past year — Target, the NSA, and Apple — the first two had nothing to do with encryption, and the third was due to a flaw in how the software handled the encryption certificates, rendering it moot. From Trojan horses to social engineering to overlooked flaws in code, there are myriad ways to access user data, regardless of the level of encryption used.

• **Encryption inspires a false sense of security.** Encryption gives you a sense that everything is okay. But it doesn't tell you who's attacking your environment, and it doesn't help you handle social attacks. Consumers will still get their green lock, but the data isn't safe to transmit.

How to put the puzzle together

Successful security comes down to a combination of tactics that work together to protect sensitive data:

• Use tools such as KSI, EMC Centera, and PKI to certify your data and guarantee that it hasn't been modified.

• Consistently review your architecture to make sure you're keeping up with known threats and vulnerabilities. Security is not a set-it-and-forget-it kind of thing; it needs to be up-to-date at all times.

• Train your employees to be on guard. Social engineering is more effective than technical prowess. In fact, your employees are your weakest link. They will be targeted and taken advantage of, and education is your only defense. Let your employees know what to look for, and ask that they never provide sensitive information to unknown or unverified individuals or trust software or hardware they don't know the origin of.

Consumers are going to demand change, governments will implement new laws, and shareholders will evaluate investments based on cyber risk. The cyber threat landscape is new and growing, and investment in technology and education is key. Not relying on any one technology to save your business is paramount. A fully formed strategy is the epitome of proactive customer care. Make sure your business is willing to invest the time and money to demand quality solutions to protect your customers.

It only takes one mistake to lose the trust of your customers. Stay informed and on top of your business' security solutions to ensure the happiness and cyber safety of your customers — and prevent yourself from becoming a Target for cybercriminals.