Stepping up to Trustworthy

The value of trust

Every day your customers are confronted with stories about data breaches and the loss of personal information. In many cases, the danger to their lives is secondhand. Information about where they live and who they are can be used by criminals to steal from them and rob them of hard-won assets. However, to execute the actual theft, the thieves need to utilize the stolen information for further attacks.

Over the last few years, your customers have been inundated with advice and tools that enable them to defend against those sorts of attacks. Increased security programs on their personal devices and new procedures to follow to make sure that those devices closest to them are safe are common.

Antivirus, Anti-malware, scanners, and firewalls. This is the shape of the new cyber landscape. For businesses, it's hard enough to keep up, and they actively employ a myriad of people to perform necessary tasks to keep their information private. Your customers must protect themselves on the Internet, or they risk ruin.

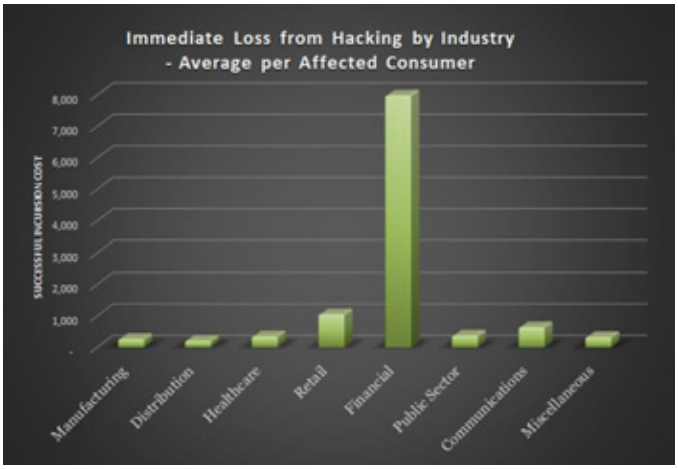
We are getting better, but the scope and the reach of the hacking attacks are growing faster than any one person can manage. So, you try to do what you can, protecting and isolating certain aspects of customer information and attempting to strike a balance between being active and safe in the interconnected world.

Some people overlook the peculiar vulnerabilities that are related to safety and security, exposure and risk when it comes to financial data. If someone steals social media account information, they have to put together that information in a way that can be leveraged in a further attack. The thieves cannot just automatically steal the money. However, if a data breach occurs in a financial institution, your customers' assets are immediately vulnerable. Theft in this situation is frequently untraceable.

The money can disappear from their account, and recovery is either impossible, minimal, or difficult.

FINANCIAL VULNERABILITY

Banks and other financial institutions have intimate details of the most damaging information possible on their account holders. When a breach occurs within a financial institution, there is no need for a secondary attack. The access puts the successful hacker in a position to do immediate damage.



The combination of extensive personal information and the immediate possibility of theft makes a breach in a financial institution one of the most severe possible. A Solitaire Interglobal Ltd. (SIL) 2018 study gathered information from over 35 million breaches of individual data to show how damaging this type of attack can be.

The immediate impact on the customers of a financial institution is far more severe than for any other industry.

For many consumers, the choice of a financial service organization is based more on the institution's response to the changing market and the availability of features than the safety of doing business with them. While agility and features are important, it is vital that all of the transactions conducted by an organization are safe and secure.

Customers need to be able to trust an organization to protect the information that it collects from them and uses to conduct its business. If they do not protect this data, it is a betrayal of the unspoken contract between buyer and seller. In other words, being successfully hacked is extremely bad for business. Especially for financial organizations and their customers.

FOUNDATION FOR SECURITY

One of the areas that is usually invisible to your customers is the underlying IT infrastructure and processes that form the first line of defense against hacking. Unfortunately, the consumer sees only the outward signs of business operations and has no insight into the foundation that protects their data.

Although many factors can affect an organization's ability to resist hacking attacks, the biggest one is the platform foundation on which everything else is built. The differences in the underlying base can be seen by the exposure of customers using the systems built on them.

The ability to tie external results to underlying data is difficult and requires huge masses of information. SIL has the largest repository of such data available commercially and has mined that information to understand the correlation between the inside business practices and the outside effect on consumers.

SIL examined customer experience grouped by base IT architectural class to see if there was a tie between a specific type of platform and a pattern of increased or decreased consumer security exposure. The results showed a consistent pattern of increased safety for customers of organizations using the IBM LinuxONE platform.

IBM LinuxONE is a significant component in constructing a foundation for trust. Hackers are far less likely to be able to breach the protections that are necessary for digital inventory, when the foundational cybersecurity has a more stringent starting point. In fact, LinuxONE implementations report *less than 0.01%* of successful security incursions per 1000 deployed applications than other architectures.[1] This translates to safer financial transactions and more protected Internet experience.

In the case of security in cyberspace, the platform matters.

SOLITAIRE INTERGLOBAL LTD.

Solitaire Interglobal Ltd. (SIL) has been gathering data on market evolution and production behavior for over 40 years. Supporting more than 6,000 clients and performing over 100M predictive models each year, SIL has also run the Global Security watch for the last 22 years. That member service has allowed SIL to build a repository that exceeds 550 PB of data at a very granular level. That data is mined every hour for trends, comparisons, and threshold that help organizations succeed.

ATTRIBUTIONS AND DISCLAIMERS

This document was developed with IBM funding. Although the document may utilize publicly available material from various vendors, including IBM, it does not necessarily reflect the positions of such vendors on the issues addressed in this document.

01020201USEN-00

[1] Solitaire Interglobal Ltd., *Scaling the Digital Mountain*, (2018, All Chaos Press)