TAKING CYBERSECURITY SERIOUSLY

Whitepaper

Let's talk. Cybercrime- what threats do you face, and what can you prevent?

USA | Costa Rica | India

info@feuji.com

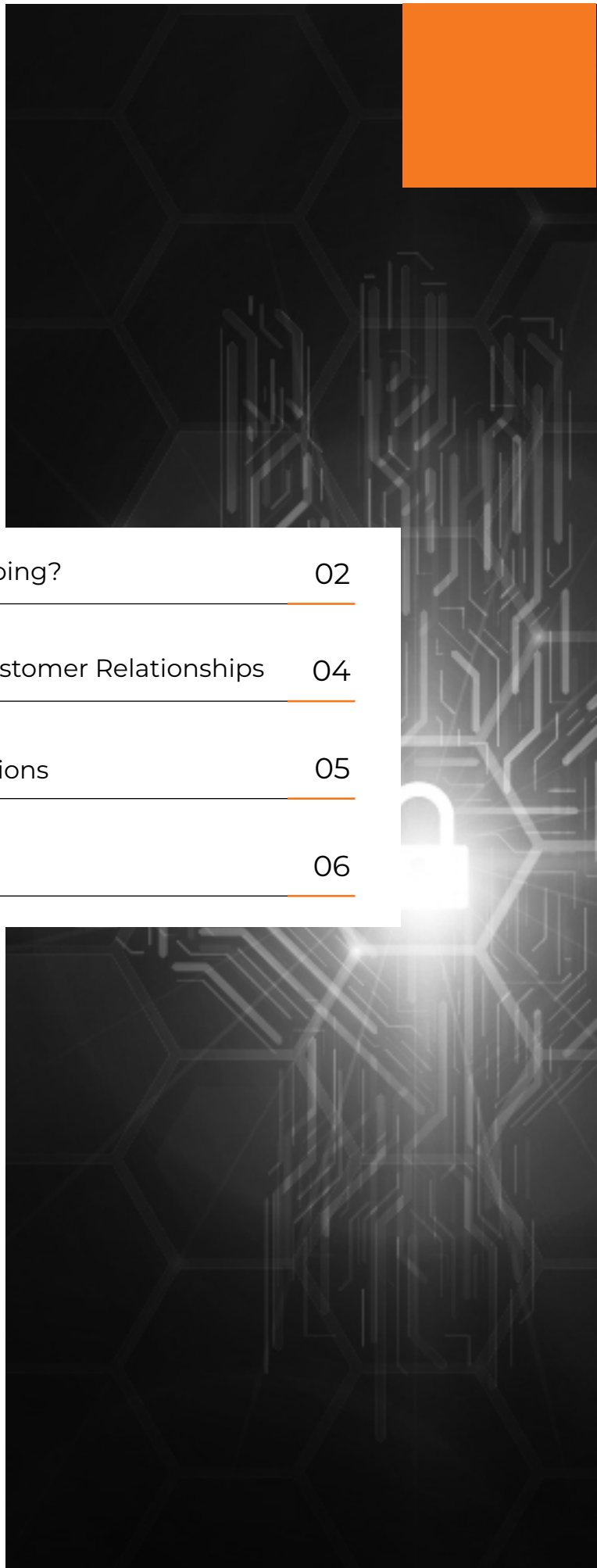

Table of Contents

What are the ‘Good’ Organizations Doing?

It is true that some organizations are taking this issue seriously and not neglecting it. Here’s how they are doing it.

Walking the Talk:

While the threats still remain, and the trends are to be taken seriously, we see that increasingly companies are making this a significant priority to be addressed. Organizations that have already experienced a crime are aggressively pursuing solutions that can fix their problems.

The Growth of Cybersecurity:

Cybersecurity is an ever-growing, ever-expanding risk mitigation defense system with humans and machines working together to combat it. There is greater awareness and better education available on this. There are a wide variety of ready solutions that can address the specific pain points of organizations and enterprises— based on their requirements and budgets.

Board Room Priority and Engagement:

Your customers are likely to lose trust in the wake of cybersecurity becoming a real and serious concern irrespective of your company being B2C or B2B—if you become a victim.

Cybersecurity is quickly becoming a boardroom priority. Here are 5 statistics that you must consider and talk about in your board rooms, meeting halls, cubicles, and break rooms alike.

“Threat is a mirror of security gaps. Cyber-threat is mainly a reflection of our weaknesses. An accurate vision of digital and behavioral gaps is crucial for a consistent cyber-resilience.” – Stephane Nappo

Data Protection and Its Impact on Customer Relationships

Trust is an essential element of a customer relationship. Cyber-attacks are a major risk for any business and could potentially lead to loss of customers, losses in sales and profits, difficulty obtaining financing for the business, and damage to the organization's reputation. It can take years to rebuild trust once it has been lost. With more businesses moving to a fully digital model, today's organizations have become increasingly vulnerable to data breaches.

For most companies, protecting the data of their employees, customers, suppliers, and other key stakeholders is the top priority. As a result, they are becoming increasingly aware that they need to have an incident response plan in place that will ensure they can quickly recover from disruptions to their business caused by outages, cyber-attacks, and data theft.

Business Disruptions and Its Implications

As a result of business disruption, and a dip in profits, organizations are becoming progressively more engaged in cybersecurity. Cybersecurity is no longer an IT problem or concern, but it has become a business and leadership issue in which everyone must engage.

Cybersecurity is one of the top 4 challenges, according a global board survey by McKinsey.

01 In the B2C world, **<50%** of customers want to share their data with any other industries than financial and medicare due to probable privacy problems

02 In the realm of B2B, **87%** of corporations would not want to do business with another organization if they don't see sufficient security protocols in place

03 Nearly **70%** of US citizens want their data to be private and state that data privacy is extremely important.

04 Only **28%** of US citizens are comfortable sharing their data with a highly regulated industry, or companies with headquarters in trusted governments.

Source: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

The board of directors and the executive leadership need to engage in a critical conversation. The board's responsibility is to make sure that the executive team has a plan, is prepared, and is preparing the whole organization for the eventuality of an attack. If a company has a plan in place, they are more likely to weather the effects of a cyber-attack. The plan should be developed by the executives and presented to the board for final approval. Expectations should be set and communication channels clearly defined in advance so that everyone knows their roles and responsibilities during an inevitable crisis.

The modern enterprise relies on data-driven insights for business advantage and competitive differentiation, which makes the enterprise vulnerable to the risk of malicious attack. The first step in mitigating this risk is to build a foundational cybersecurity capability that can detect, control, contain, and remediate incidents at a pace and scale that keeps up with emerging threats.

What Solutions are Out There?

According to a McKinsey report, the 4 key capabilities that are needed to mitigate cybersecurity risks related to on-demand access to ubiquitous data and information platforms are

01 **Zero-trust capabilities**

01 **Behavioral analytics**

01 **Elastic log monitoring**

01 **Homomorphic encryption**

We will go over each of these solutions in detail.

01

Zero-Trust capabilities

Hybrid and remote working have dramatically increased during the pandemic. And along with this has increased cloud access and Internet of Things (IoT) integration leading to an increase in vulnerabilities. The nature of threats and the way they are carried out has changed dramatically over the past decade.

The traditional perimeter-based approach to cyber-defense is no longer sufficient, as it focuses on defending static perimeters around networks, thus leaving data and users vulnerable. A zero-trust architecture mitigates the risk of decentralized data. Zero Trust is a layered approach to cybersecurity that assumes that any access to a network or system should be considered hostile, whether it comes from a valid user or not.

The secret to a successful zero trust strategy is to prioritize security over convenience. To achieve this goal, enterprises must rearchitect their networks to address the two primary factors behind today's widespread cyber threats: privileged access and the need for identity federation across internal and external environments.

02

Behavioral Analytics

Analytics provide the means to integrate cyber and physical security. The best-in-class analytics solutions continuously monitor attributes such as user and device access requests, or the health of devices to establish a baseline.

Analytics solutions monitor user activity patterns and normalize them against behavioral baselines to identify anomalous behavior, enabling quick action and mitigating damage. Risk-based authentication and authorization are supported by these solutions, as are preventive and incident response measures.

03

Elastic Log Monitoring

With the abundance of data produced by systems such as big data and IoT, it is no longer sufficient to only store logs centrally or to rely solely on periodic manual analysis. More advanced approaches are required to monitor activity in real time and at scale while also providing actionable insights. As companies expand their use of big data and the IoT, they face a growing log-monitoring challenge. With the large volume of time-sensitive events they generate, log data can overwhelm tools that traditionally have been used to monitor IT infrastructure.

Elastic log monitoring addresses this challenge with a solution that combines open-source platforms to aggregate log data from anywhere in an organization into a single place and then enables real-time analysis and visualization. This allows users to quickly identify anomalies and threats that may otherwise go undetected for days or weeks.

04

Homomorphic Encryption

One of the biggest challenges facing the analytics industry is handling sensitive data that cannot be exposed in its raw form. Homomorphic encryption addresses this problem by enabling companies to safely share data without having to decrypt it first. This means that cloud providers can host extremely sensitive data and perform computations on it without ever decrypting it, giving third parties and internal collaborators safer access to large data sets while helping companies meet more stringent data privacy requirements.

In our next white paper, we will discuss more about the solutions available to combat increasingly sophisticated cyber-attacks.

You can go to www.feuji.com/contact and enter your details so we can send you information that matters.

CONTACT US

USA | Costa Rica | India

info@feuji.com