TRENDS IN CYBERCRIME

Whitepaper

With multiple trends and types of cybercrime, how do you stay prepared?

USA | Costa Rica | India

info@feuji.com

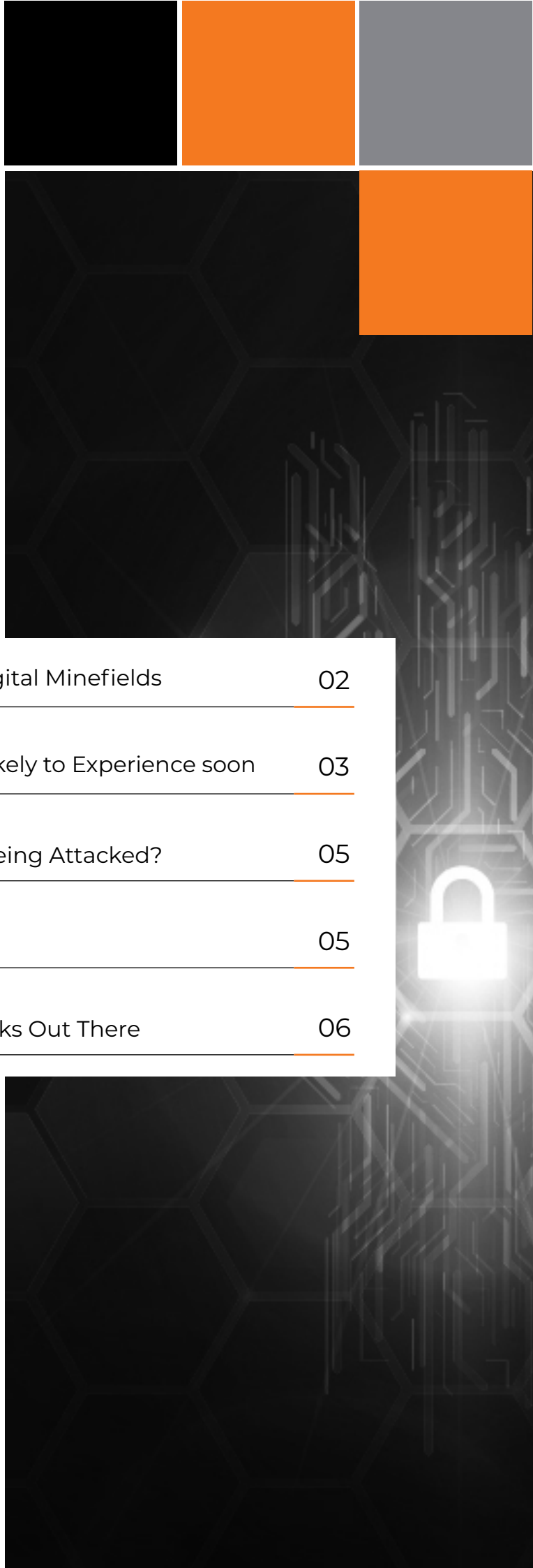


Table of Contents

Digital Landscapes are Becoming Digital Minefields

In our previous whitepaper, we discussed at length about how the digital landscape is becoming a digital minefield. Yes, the digital revolution is changing the world. Yes, organizations have become increasingly agile and innovative. However, in the face of these changes, teams are dealing with the pressure to protect sensitive information. The widespread adoption of DevOps strategies is leading to increasingly frequent deployments and updates. This has an impact on cybersecurity.

Here are five important statistics you must consider and ponder upon before we move forward:

With AI and sophisticated tech involved, just in 2020 alone, We saw nearly **150% more phishing and ransom ware attacks.**

Organizations must, therefore, balance the need for speed with security requirements.

Ever since the late 1980s, there have been systematic cybersecurity threats that affected organizations. To this day, it is still a problem and places new vulnerabilities. The threats are more intense, sophisticated, and growing. There is a growing trend where hackers are incentivized to develop large-scale hacking capabilities. It has become an industry of its own.

With those staggering statistics in mind, there are three key trends that a McKinsey report suggested, which could have large-scale implications:

According to a Gartner report, companies might need to pay up to **15X more than the ransom** for the cost of recovery and the resulting downtime in the aftermath of a ransomware attack.

According to a Gartner report, **45%** of organizations across the globe would have experienced attacks on their software supply chains in 2022.

There has been a **300% increase** from 2021 to 2022 in the amount of ransom ware related cyber-crime according to this Gartner report

53% of companies had **over 1,000 sensitive files open** to every employee according to this report

Cyber Security Trends that You are Likely to Experience Soon.

01

To understand and influence purchasing behavior and to forecast demand, organizations have been collecting a lot of data about their customers. Just during the COVID crisis of 2020, even more data has been gathered. Every second, each human on planet Earth created 1.7 megabytes of data.

The data is not only gathered and stored on the cloud (for the most part) by organizations but access to the data is granted to others, including third parties. APIs, often combined with vulnerabilities, access this data. Eventually, data is compromised internally or is exploited by attackers.

There is a growing trend to protect this sensitive information—to the point where **governments are having to regulate the means by which data access is protected, shared, and saved.** Unfortunately, despite the use of these regulatory measures, we are still experiencing the growth of cyber crime. Not a dip in it. There is always a back door.

02 Advanced technologies used by attackers

Today, cyberattacks are increasingly sophisticated and stealthy. They are quite literally, automated. AI is being used, and so is machine learning, and a whole host of other advanced tools and techniques, to launch sophisticated attacks on businesses.

Cybercrime is a million-dollar enterprise. Although billions are being spent to overcome it, it is insufficient.

Ransomware, phishing, malware, and exploitation of sensitive data is just the beginning of cybercrime. As we see an increase in the use of other technology for malicious purposes, we will see this threat becoming a greater reality that we should all be concerned about, personally and at work.

It is forecasted that in the next several years, the attackers will be able to expedite all the way from reconnaissance to exploitation from weeks to days or hours. This means that in a few years, advanced technology will be able to infiltrate your private infrastructure and data in just a few hours if you don't take the right measures.

03 Insufficient cybersecurity expertise

There is a great gap between the ever-widening incentive to cybercrime, versus the cyber policing we have in place today. Like we explained before, cybercrime is a multi-million, if not a multi-billion-dollar business. But we need to take an honest step back and think about where this all started, especially in the age of the cloud.

Organizations place more emphasis on digital transformation and analytics. As a result, cyber risk management has taken a back seat. While organizations admit the risk of cyber-crime, there is not enough being done. And that is because more and more human talent is being utilized to develop digital transformation, cloud technology, automation, AI, and a whole host of other technologies.

As a result, the incentive for human talent to sincerely develop cybersecurity systems is reducing. The identification and management of digital risks is proving to be an uphill task for many organizations. Adding to the challenge is the ever-growing regulatory landscape. There has been a steady increase in the guidance of corporate security capacities by the regulators. Organizations follow a wide range of policies like ISO, GDPR, HIPAA, etc. But the expanded access to data presents risks for which we do not have a one-size-fits-all solution.

How do You Stand a Chance of not being Attacked?

Any organization with a computer network connected to the internet is susceptible to cyber risks, from single offices to large multi-site organizations. This is where business leaders and key decision makers must get involved and look for ways and means to prevent the occurrence of these attacks. There is a deep reason why CEOs must consider bringing in CTOs and building teams or engaging consultants to help prevent these malicious threats and attacks.

Questions You must Start With

You need advice on what to do in the instance of an attack. To begin with, you should ask yourself these questions:

- How do you get started seriously taking action in your organization?
- Do you have the right firepower and infrastructure to combat this?
- What can you do to reduce the impact cybercrime has on you?
- Where do most (or all) of your risks lie?
- How are you going to plan for a “what if” scenario?
- What will you do if someone in your organization passes information to external parties?
- What can be done to help mitigate risks?
- What are some policies that you can implement internally?
- What will you do in the instance of someone external infiltrating your infrastructure?
- What are compliance norms you should embrace?

The Most Common Cyberattacks Out There

Although this is just the beginning of an extensive list of the forms and types of cybercrime attacks out there, your board and executive teams should know which are the most common ones and take necessary action.

With that in mind, let us look at the most common means of cyberattacks. Some of the most common cyberattacks according to Gartner are:

"One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks. Fix the basics, protect first what matters for your business, and be ready to react properly to pertinent threats. Think data, but also business services integrity, awareness, customer experience, compliance, and reputation."
– Stephane Nappo

Ransomware

Ransomware is increasing in frequency and severity, making it more important than ever to ensure that your organization has the information it needs to combat this threat. Ransomware has become an increasingly popular way for hackers to make money. It quickly paralyzes entire organizations and inflicts millions of dollars in losses. It is a big threat to businesses causing failure to restore systems in a timely manner- resulting in financial loss, lack of trust from customers, lawsuits, fines, penalties, and more.

Phishing and unauthorized access

Phishing is a type of fraud that uses social engineering to trick people into revealing confidential personal and financial information, including passwords and credit card numbers. It often takes the form of an email containing a link or attachment that leads to a fake website designed to look like a legitimate business. Phishing opens doors for data exfiltration. Because data exfiltration is stealthy and takes place over time, it can be particularly hard to detect. Attackers can steal enormous amounts of sensitive data without anyone noticing.

Supply chain attacks

Software supply chain attacks are one of the biggest security threats in businesses today. They can steal private data, or damage software by inserting malware into a development process. The goal is to gain access to source codes and build processes by infecting legitimate apps or updates with malware. After breaking into an app's server infrastructure, attackers change the targeted software and hide malware in build and update processes. These attacks could be dangerous because they are hard to detect and use legitimate apps to spread malware.

Denial of service (DoS) attacks

The DoS attacks are a common way of disrupting an organization's network, causing a temporary shutdown or slowdown. DoS attacks can occur on a networked computer or server via a flood of network packets, which overwhelms the target's ability to process data. The attack prevents legitimate users from accessing their services or resources by flooding the target with more traffic than it can handle. Since many of these attacks target web servers of high-profile companies, they can also bring down sites that are critical for customers to access.

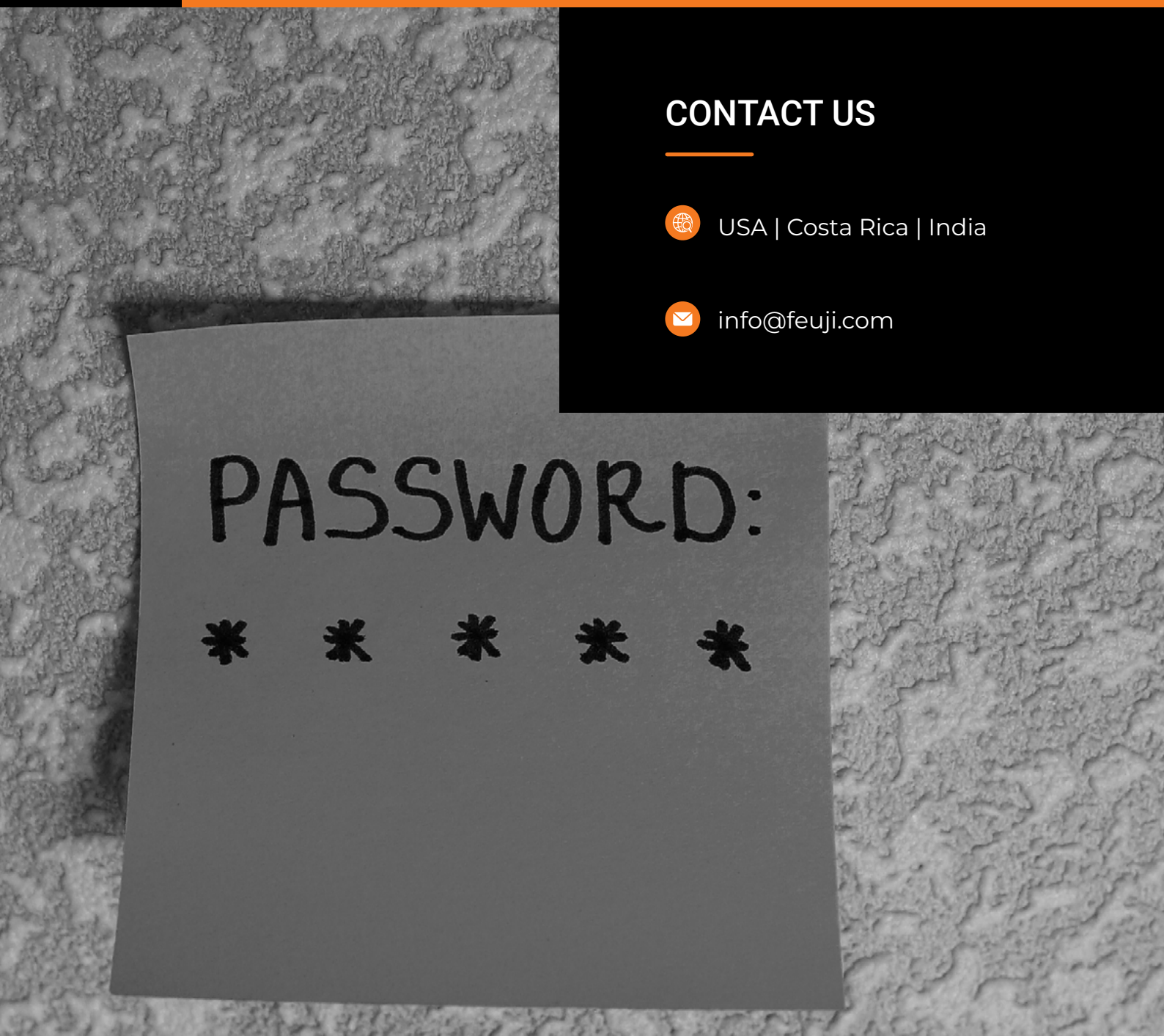
Cyber Account Compromise

Criminals regularly target organizations for the passwords to their accounts. They use hacking techniques that enable them to identify common and reused passwords, which can be used to gain access to confidential systems, data, or assets. The proliferation of password-related compromises has become a costly and widespread problem for IT. These attacks take place at random, from all corners of the globe, and target big companies as well as small businesses. When unauthorized users gain access to an account, they may steal critical data or disrupt operations. They may damage the brand name or tarnish an organization's reputation by broadcasting false messages in the company's name. They might even delete everything on servers within minutes and cause irreparable harm to the company.

Eavesdropping on unsecured network traffic

By not taking actions to properly secure network traffic, an organization exposes itself to a variety of threats. Network-related and man-in-the-middle attacks can pose a serious threat to the security of an organization. Attackers may be able to eavesdrop on unsecured network traffic or redirect or interrupt traffic. This can allow them to impersonate users, intercept credentials or client-side sessions, corrupt data, or disrupt the system.

There is so much more we can share. But we understand that you only have limited time to read. To read more about this threat, and to take action that is relevant to your company, read more about this topic in our subsequent research presented through our whitepapers. Reach out to us via email: info@feuji.com so we can send you information on how to combat this.



CONTACT US

USA | Costa Rica | India

info@feuji.com