feuji

CYBERCRIME— DIGITAL MINEFIELDS

Whitepaper

Today's digital world faces increasing cybercrime. How do you prevent it?

USA | Costa Rica | India

info@feuji.com

Table of Contents

Anyone can fall victim to cybercrime and any computing device can be infected with malware. Nobody is immune to cybercrime”
– Amanda Jane Turner

The Inevitable Present and Future

Digitization has become a natural, imperative evolution for nearly all organizations today. Organizations have moved away from the industrial age, when they were primarily focused on performance and efficiency, to a model in which innovation is the primary goal. Information and Communication Technology (ICT) has become ubiquitous in companies.

It is ICT that is driving the third industrial revolution, which is characterized by an increased reliance on big data and cloud computing systems. Cloud-based systems enable companies to quickly collect and analyze data, provide real-time information, interact with customers, and improve operations.

Cloud computing provides access to applications or infrastructure as a service, thereby enabling organizations to break down silos, integrate new systems with legacy technology, and increase their speed of innovation and responsiveness to market needs.

In the past few years, we have also witnessed an unprecedented rise in the quantity and sophistication of cyberattacks. This threat is not going away but only getting worse and more complicated to prevent. Here are five worrying trends.

At this point we want to bring to notice three factors that you should be concerned about.

A How is cybercrime becoming an industry of its own?

B How well are organizations prepared to combat this threat?

C What kinds of organizations fall within the scope of cybercrime?

We will briefly answer these three important questions.

In the past few years, we have also witnessed an unprecedented rise in the quantity and sophistication of cyberattacks. This threat is not going away but only getting worse and complicated to prevent. Here are five worrying trends.

The world-wide spending on thwarting cybercrime is nearly $134 billion in 2022

70%
of company leaders feel that the risk of cyber-attacks on their organizations are more and more likely to happen

Only **5%**
of companies worldwide are properly protected. The remaining 95% are vulnerable because of sheer negligence and the lack of security protocols

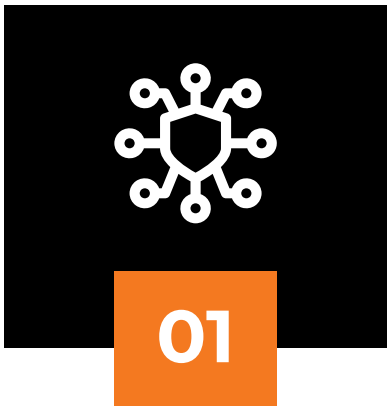
Every
32 seconds
hacker attacks someone online. That is about 2500 attacks each day, across the world.

At most companies, most breaches go unnoticed for over
200 days
With hackers becoming increasingly powerful, that number is increasing

Source: https://legaljobs.io/blog/cyber-crime-statistics/

The Industrialization of Cybercrime

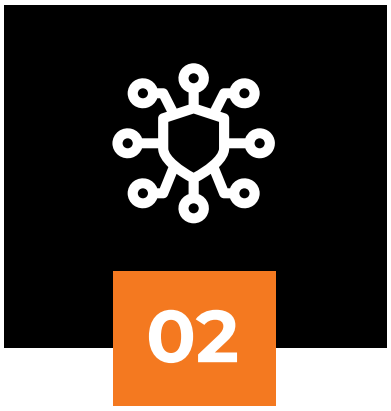
McAfee, one of the world's most trusted cybersecurity experts, is dealing with a problem worth $400 billion. Simply put, the evolution, and the pace with which cybercrime is growing is giving organizations, and even governments more than they can deal with and handle on their own.



01

Cybercrime as an Industry:

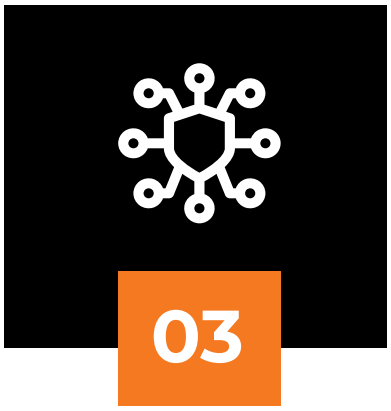
According to one McKinsey report, cybercrime is becoming industrialized. Vulnerabilities are identified by one set of groups, who then share the information with criminal groups. These criminal groups lease ransomware in exchange for a percentage of the profits and employ it against victims.



02

Results:

The results are both expensive and damaging. It is extremely complicated to identify and reduce the possibility of an attack. Enterprises of all sizes, businesses, and even governments, are being put to the test of industrialized cybercrime.



03

Incentivized crime:

Recently, the Wired magazine indicated how it is almost entrepreneurial to become a hacker. "The opportunities are high, and the risks are low", the magazine quotes. What an incentive to be an agent who thrives by committing cybercrime!

The Lack of Preparation

01

Negligence:

Imagine going to war, but without the requisite artillery. There is a reason why most armies are called a country's' "defense" instead of "offense". Much alike, cybercrime is a war we need to fight. We need defense and preparation to combat these cyber threats and cyber risks. This is a minefield. It is literally cyber warfare.

02

Indiscipline:

But there is a woeful problem as well. That is the condition of a lot of enterprises, businesses, and governments today in the context of cybercrime. Risk mitigation methods that can combat cybercrime to a significant extent are mostly unknown or even when known, they are seldom followed.

03

Threat readiness:

Brands and countries, organizations and enterprises, governments, and businesses are not prepared to combat cybercrime simply because they are not as serious about it as they should be. It's unfortunate, but true.

Most countries have more people allotted for nuclear arsenal than cybercrime combat. The lack of preparation for cybercrime (even though it is noticed, and mature) is an unfortunate risk most countries, governments, and companies face, but severely underestimate.

Even The Onion Router (TOR), created by the US Government and later released to the public, cannot spare an organization. The United Nation's Office on Drugs and Crime had to get involved in preparing organizations to combat cybercrime. Their website states "Tor and other anonymizing networks have also been utilized by cybercriminals to commit and/or share information and/or tools to commit cyber-dependent and cyber-enabled crimes".

Will Your Company Face Cybercrime?

The short answer: Yes. The probability is very high.

01

The big fish: Codespaces, The Heritage Company, Travelex, MyBizHomepage, Wood Ranch Medical, Youbit Crypto Currency Exchange. All these companies have fallen prey to criminal cyber-attacks, gone bankrupt, and even shut down. No one really knows the number of smaller companies that went bankrupt because of cybercrime

02

All the fish: Big ones, small ones, mediocre ones, and even government agencies are being toppled by cybercrime. In all cases, no one knows who it was that committed the crime. The anonymity is the incentive that allows hackers to plan and execute their cyber-attacks.

03

How deep this goes: Cybercrime, as we explained above, still has a heavy load of power to take companies down, and even bankrupt them. They can modify how people think just around election time, while even compromising private government email transactions— not to mention exposing private pictures and videos of normal citizens like you and me.

Cybercrime even tried to manipulate the public in the United States ahead of elections. Most recently in 2020 and 2021, Israeli and Indian governments were targeted by a wide range of cyber terrorists from several countries. Within just one week, the Indian Ministry of Electronics and Information Technology was compromised not once, or twice, but three times. Hackers accessed confidential emails of several top officials in the Indian government.

01

What's the response like? McKinsey reports that many companies, (and as we see, even governments) are not sure how to identify and manage cyber risks. The management of cyber risks has not kept pace with the spread of digital transformation. As companies explore opportunities in the rapidly evolving digital economy there is serious necessity for plucking out negligence.

02

Who is being attacked? Cyber-attacks are no longer rare or the domain of large businesses. Small and medium-sized organizations are increasingly being targeted, and they must change their current cybersecurity approaches to address this new reality. More and more, these threats are becoming prevalent, dangerous, and serious. Most often, decision makers and key leaders in organizations are being targeted.

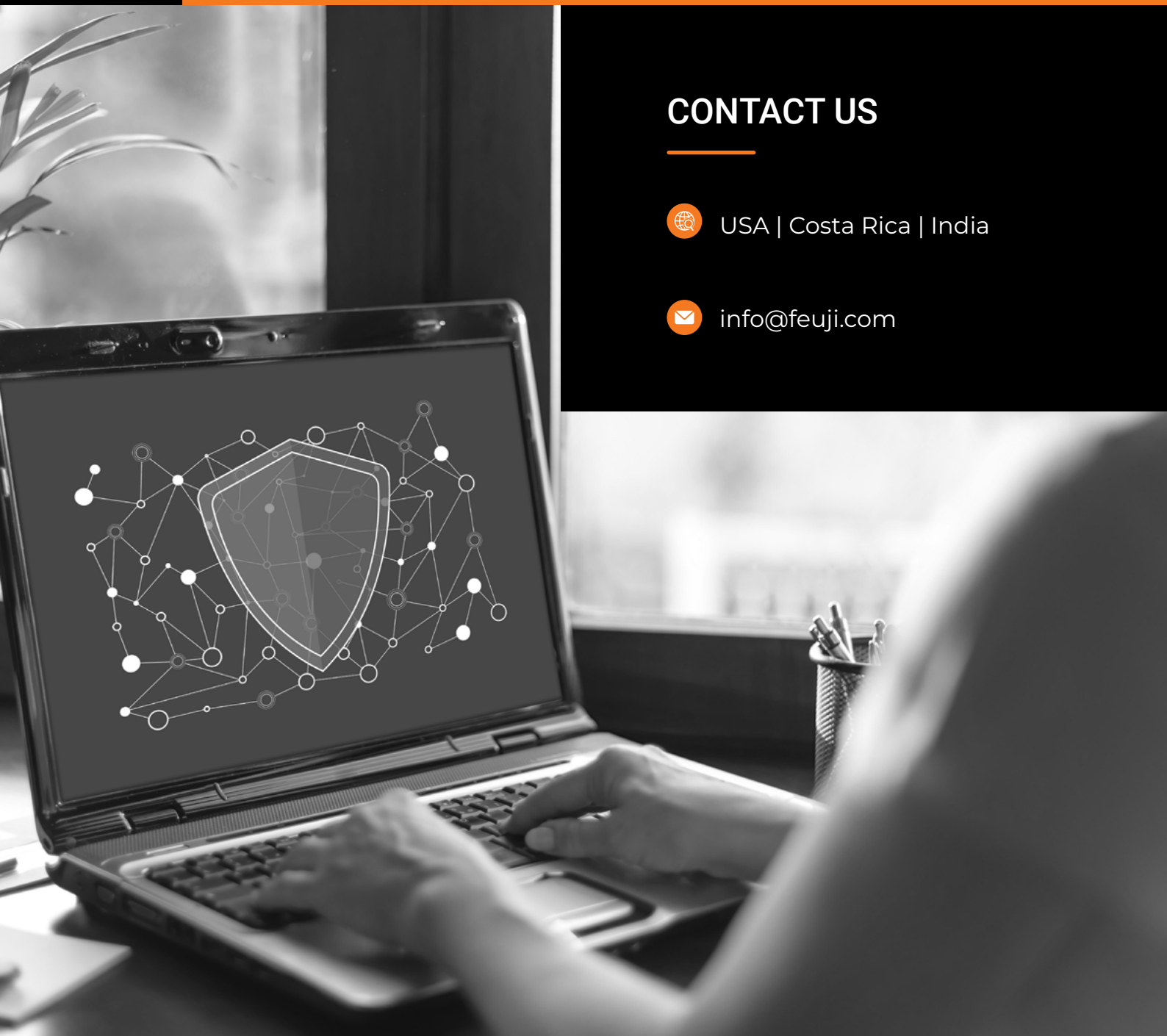
03

What must we do? The key to planning for a cybersecurity incident is learning from the past, anticipating what may happen in the future, and crafting plans and exercises to prepare so that we are ready when it strikes, no matter how unlikely that scenario may seem. We need to find ways to provide access to data, while ensuring that it is not hacked through internal security vulnerabilities. We need to be prepared to redefine the way we manage data in this new digital landscape.

Our Conclusion

Cybersecurity is a threat and a genuine risk for your organization that must not be ignored. We're not trying to scare you.

But this is the posture and preparation your organization must take while facing the reality of cybercrime that's out there. You can read more about the trends in cybersecurity in our subsequent whitepapers.



CONTACT US

USA | Costa Rica | India

info@feuji.com