2019 IN CYBERSECURITY

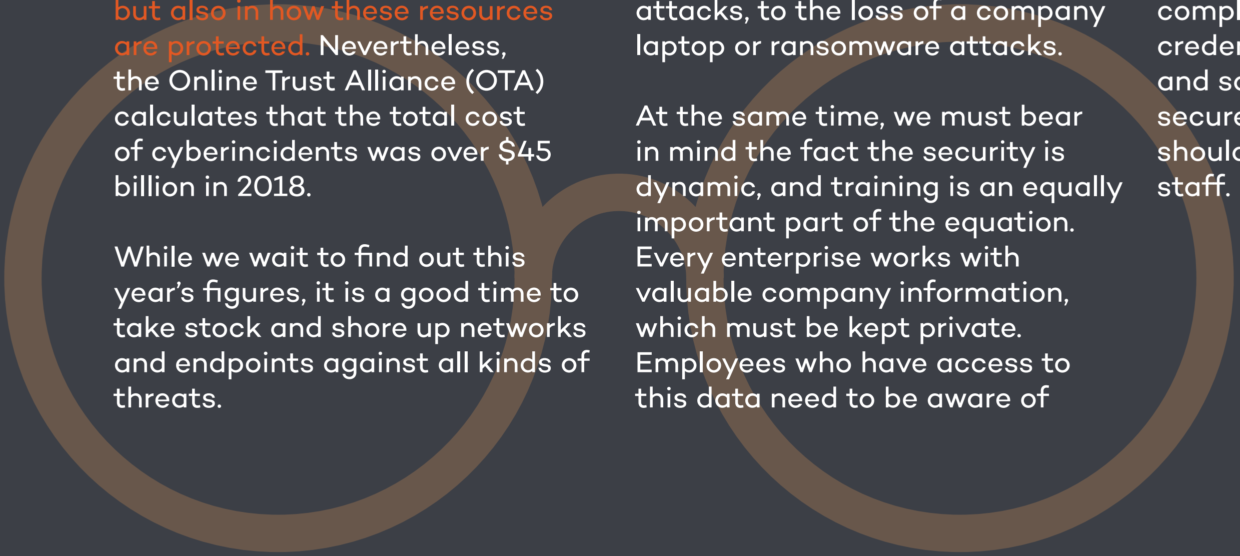
THE EXPERTS TALK

panda

pandasecurity.com

INDEX

PROLOGUE



On International Computer Security Day, and with the end of the year just around the corner, we take a look at some of the unfinished business that enterprises still need to tie up when it comes to security.

Organizations' against-the-clock race to digitalize should be reflected not only in the implementation of technologies, but also in how these resources are protected. Nevertheless, the Online Trust Alliance (OTA) calculates that the total cost of cyberincidents was over $45 billion in 2018.

While we wait to find out this year's figures, it is a good time to take stock and shore up networks and endpoints against all kinds of threats.

In spite of the fact that a cyberattack can have a devastating effect on a company, the vast majority of enterprises are not prepared to deal with a problem on this scale. Even if we have a foolproof prevention plan and a stellar team, breaches happen. This is when we need a good incident response plan in place: from dealing with new tactics like Living-off-the-Land attacks, to the loss of a company laptop or ransomware attacks.

At the same time, we must bear in mind the fact the security is dynamic, and training is an equally important part of the equation. Every enterprise works with valuable company information, which must be kept private. Employees who have access to this data need to be aware of how important it is, along with the fact that protecting it is their responsibility. The human factor is still the common element among most cyberattacks. With this in mind, companies cannot afford to skimp on their IT security training budget for programs for their staff.

Though it may seem logical, guidelines such as choosing complex passwords, not reusing credentials on different platforms, and saving this information in a secure place, are behaviors that should be habitual among the staff.

The long-awaited creation of a common digital framework finally came with the appearance of the European General Data Protection Regulation (GDPR). A year after its implementation, 30% of European companies still are not compliant with the rules laid out by the GDPR. This exposes them to the risk of incurring steep fines from the authorities, as well as a loss of customer trust.

Finally, along with increased security for corporate networks, a cyberattack response plan, investing in training and adapting to the demands of the GDPR, reducing alert fatigue in IT security teams with automation technology and advanced services is still a pending subject. An increasing amount of security alerts and the shortage of professionals can overwhelm cybersecurity teams, and cause them to overlook the signs of a possible attack.

Do the experts behind our guest posts this year agree?

Enjoy our compilation, “2019 in Cybersecurity. The Experts Talk”.

Marta Zapata

Global Communication Manager
Panda Security

Román Ramírez

THE WEAK POINTS OF CYBERSECURITY ARE PEOPLE AND INVESTMENT

Román Ramírez is very well known in the world of cybersecurity in Spain. The founder of RootedCon, the most important security event in Spain, and with over 20 years of experience in the sector, he has been Manager of Operations and Security Architecture at Ferrovial for ten years. In this company his role is to manage security operations at a corporate level, as well as to manage security for projects and new developments within the organization. We have arranged to talk to him about corporate cybersecurity in large and small companies, cyber-resilience, and cyberattack trends among other things.

Do Spanish companies do enough to protect their cybersecurity?

It's a complicated question. An IBEX 35 company whose main line of business is related to the financial sector will, of course, have more adequate protections for their assets and a much higher level of cybersecurity. On the other hand, a one-person SME in the construction industry is likely to be on the other end of the scale. In general, companies have the level of cybersecurity that they themselves have planned (that is, that they've decided on), though there are areas where, for reasons of cost or culture, there is a lot of room for improvement.

Is there at least a bit more awareness of cybersecurity?

Right now, cybersecurity is mainstream. Every day there's something in the news about it. If that doesn't make people more aware of cybersecurity issues, what will? In my opinion, awareness training is only effective for people who are already up to speed; we all know what people are like. If we need to get over an obstacle in order to achieve a goal, that's what we'll do. No amount of awareness training is going to change that.

Do you think that the GDPR will make companies take better care of their cybersecurity? Or will we see a myriad of companies being fined for breaching the regulation?

I think that it's easier to comply with the GDPR than it was to comply with the previous LOPD (Ley Orgánica de Protección de Datos de Carácter Personal – the predecessor of the GDPR in Spain). We're moving towards a more "Anglo-Saxon" model, where you'll be asked for a posteriori guarantees (with proof). I think this is going to help it to spread. And I do think that, with the growing concern for privacy, we're definitely going to gain something in several different areas. As for the fines, given how hefty they can be, I have a feeling that they're going to be very cautious when it comes to handing out sanctions.

What are some possible weak points that companies may have?

They're always the same: people and investment. Cybersecurity in any environment is intricately linked to the level of investment. If you have appropriate investment (economic and human), you'll have an appropriate level of cybersecurity.

“Cybersecurity is mainstream”

Every day there's something in the news about it. If that doesn't make people more aware of cybersecurity issues what will?

Is it possible that there is a lack of cyber-resilience?

I think it's very possible, and it does in fact happen. You might not let your guard down, and you're always vigilant for threats... And then you face a situation that's difficult to manage, and where it is hard to be resilient. The trouble with cybersecurity is that it is an environment where there are no predictable 'positive' rules (there are plenty of negative rules: if you don't invest, I can guarantee you that you're going to have some serious problems). Investing and properly managing security is no guarantee that nothing is going to happen to you. And if something does happen to you, it's tricky to anticipate outcomes and consequences.

For years, companies always had a reactive attitude to attacks. Are they becoming more proactive? Or do they still wait for some kind of catastrophe to befall them before they take action?

Companies that take security seriously systematically test their assets, infrastructure and staff. With Red team processes, constant revisions, threat modelling... it's unusual to come across organizations that still think reactively.

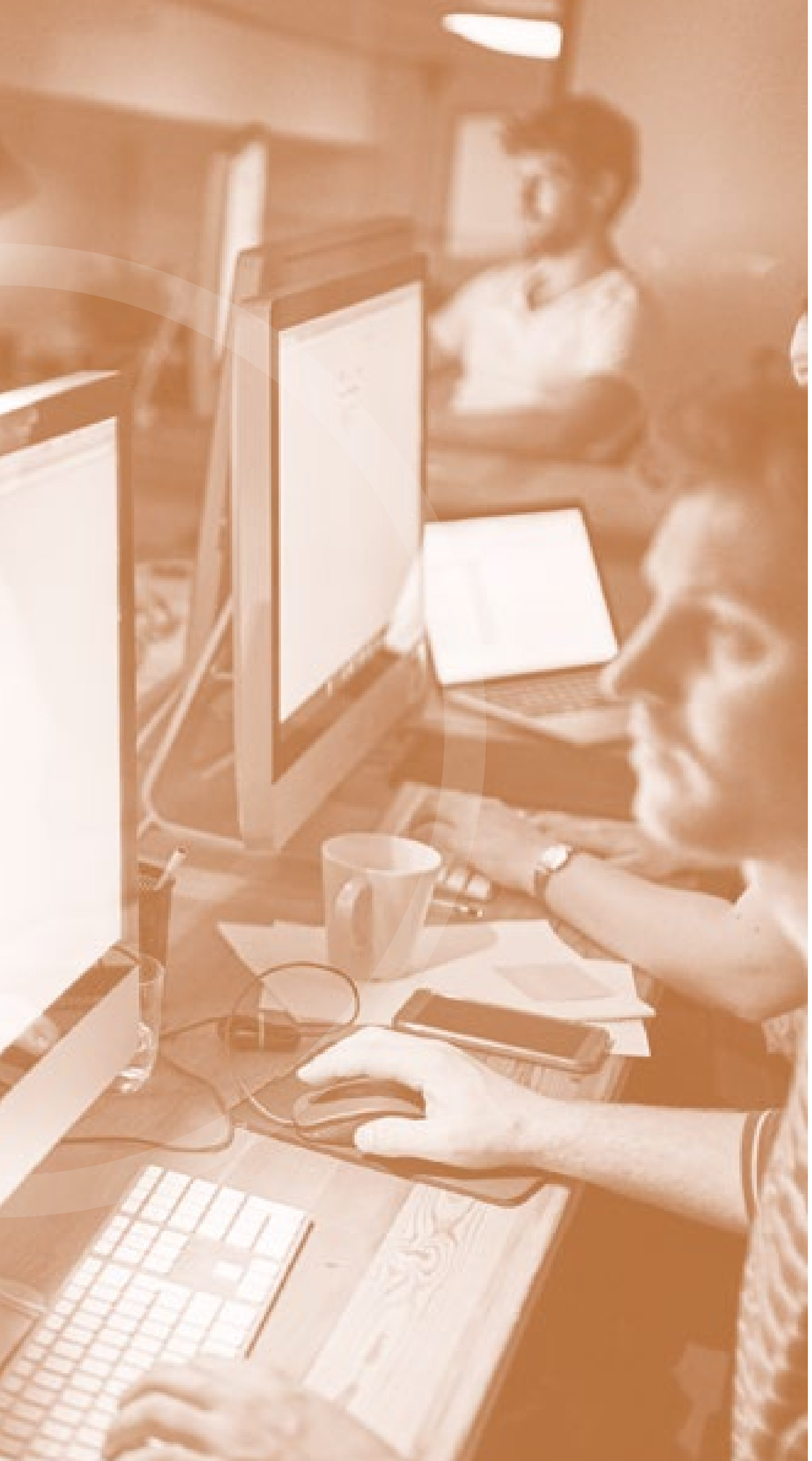
What cyberattack trends do you think are the most worrying these days?

Where we're seeing a particular increase is in everything that is less technical and more industrialized: a lot of phishing campaigns, a lot of cryptomining... Despite the consequences that they can have, cryptolockers aren't the most dangerous thing out there these days. I see the boom in artificial intelligence techniques as something that could enhance the tools used by cybercriminals, which will make defending against their attacks more complex: there's going to be a lot more automation with even more capacities and abilities.

One thing that I find particularly worrying is that intelligence agencies, where traditionally they were going after bigger targets, have been working on our more mundane level for years now. This is having more and more consequences for businesses, as well as for citizens.

Imagine you've the boss of a SME with 50 employees in front of you, who says that cybersecurity concerns don't affect him, since his company isn't important enough to be attacked by anyone. What would you tell him?

That he's living in a parallel universe and riding happy unicorns, and that it might be a good idea for him to analyze whether, in order to avoid feeling the pressure of the investment that his company needs, he isn't fooling himself and taking biased decisions. Because any incident is enough to lead to a business closing down if negligence can be demonstrated, if there are consequences for third parties, sanctions from regulators, or theft of intellectual property (which means that you can be removed from the company because someone that has copied you can do it cheaper than you can) ■



Javier Diéguez

TO INCREASE THEIR CYBER-RESILIENCE, COMPANIES FIRST NEED TO FIND A RELIABLE PARTNER

One thing that has become quite clear over the last few years is the fact that cybersecurity goes beyond the purely technological: it is a set of practices. According to Javier Diéguez, director of the Basque Cybersecurity Centre, we now understand that cybersecurity involves an element of best practices and enterprise risk management. This has given our discipline a much more transversal role. Security is now taken into account as a critical factor at a managerial level in businesses, and not just as a concern for the IT department.

Javier has over 15 years' experience in the corporate and industrial security sector, and was chosen to set up the Basque Cybersecurity Centre. Diéguez also makes up part of the team of experts that collaborated with the National Center for the Protection of Critical Infrastructures (CNPIC) to help define the sectoral strategic plans for the electricity sector.

What does your job as the director of the Basque Cybersecurity Centre entail?

I was hired to create the BCSC from scratch, managing a series of short-term objectives such as organizing the centre itself and establishing relationships with other national and European agencies. I was also tasked with constructing basic services to increase the maturity of the Basque cybersecurity industry, fostering a corporate culture of protection and defense.

As well as having a particular awareness of how important it is to protect industry and to encourage competitiveness, the Basque Country has a rather important emerging cybersecurity sector. There's no other place with such a high concentration of cybersecurity startups and technology products. At the BCSC, it's our obligation to develop that ecosystem and encourage it to grow, to search for international connections and opportunities; as it is a digital business, it can't remain merely at a local level.

In your opinion, what are the most serious threats around these days?

The majority of complaints that we receive are related to all kinds of different fraud: from indiscriminate phishing to highly targeted attacks, like impersonating the CEO. In a more industrial environment, as is the economic core of the Basque Country, there are another two important types of attack. The first of these is sabotage: disrupting operations, which is less common, but can take on a lot of different forms in an industrial environment. And a second threat, one that is far more difficult to spot, is cyber espionage. This kind of attack is mainly about stealing intellectual property in order to get a competitive advantage and endanger a potential business rival, as well as stealing information about commercial strategies.

A lot of your career has been dedicated to critical infrastructure, especially electrical infrastructure. What are the most common risks that affect that industry?

Attacks on businesses were considered nigh on impossible, or at least extremely difficult, until just a few years ago. However, nowadays the systems used by critical infrastructure are increasingly connected to the Internet, opening up more points of contact with the outside, especially for maintenance work. There needs to be a high level of surveillance to make sure that the perimeter, that surface that is exposed to the Internet, is properly protected. It is also important to make sure that networks are separated within the company, differentiating between critical networks and those that are less important. In this area, there's still a lot of work to do: segmentation isn't always as it should be, perimeters aren't always well defined, and nor are they well protected against unauthorized access, either intentional or accidental.

There is also a series of problems related to the longevity and diversity of the systems and lifecycles of the systems that support critical infrastructure. The lifecycles of the systems in electrical infrastructure last decades. We see cases where systems from entirely different generations work side by side; many of them are legacy systems. It's not uncommon, for example, to come across a Windows NT 4.0 operating system, which is from 1996. Maintenance for this software just doesn't exist, and patches for these systems are no longer manufactured.

A third problem comes from the nature of the technology and the support policy that the manufacturers of the equipment have. A company like Siemens or Honeywell usually sets limitations so that their customers, the infrastructure operators, can add independent or external control mechanisms to the package of solutions that the manufacturer has sold. This limits the evolution of the protections in our environment.

How can a company increase its cyber-resilience?

Organizations need to diagnose their risk profile, and give themselves a check-up. To do this, the first thing that a company must do is to find a trustworthy partner. It is in the company's interest to choose a cybersecurity partner that is independent of the organization, guided by the company's managers, who know the business's priorities. This means that they are able to establish priorities and determine the most important assets and processes that need to be protected. Once this profile and these priorities have been defined, a company can start to take steps. There are also many basic measures that need to be applied.

- Protection for incoming emails.
- Browsing filters to stop access to malicious URLs.
- Protection for workstations with endpoint solutions.
- Regular disk backups to tackle attacks such as ransomware that encrypt the company's data ■

Juan Antonio Calles

THREAT HUNTING COULD IMPROVE DETECTION AND RESPONSE CAPABILITIES AGAINST CRYPTOJACKING

Juan Antonio Calles, CEO of Zerolynx and SCO of Osane. Before this, he worked as head of the KPMG cybersecurity laboratory, and head of the the Everis hacking center. As well as this, Juan Antonio also has several prestigious certificates, such as Certified Hacking Forensic Investigator (CHFI) from Ec-Council and CISA from ISACA.

According to this IT security expert, the last 15 years have seen a tremendous evolution. “Security jobs used to focus on revising client websites and internal auditing to evaluate the security of the employees’ IT parks. The sector has got to a point now that, back then, was very difficult to predict.”

As companies increasingly adopt cloud strategies, how can we guarantee their security?

A few years ago, many companies thought they were safe with just a firewall to protect their perimeter. But this of course overlooked the fact that it's not just external threats that need to be protected against: internal threats are just as important. Now boundaries are starting to disappear. If we add to this an amorphous cloud containing all our information, spread over several data centers all over the word, with different jurisdictions, the security environment starts to get complicated.

If we are determined to migrate to the cloud, it is vital to check whether we have the capacity to build a cloud over our infrastructure. Where possible, we have to properly evaluate possible vendors, and once decided, try to store data in an encrypted format.

The firmware of Nintendo Switch was hacked on the same day it was launched. How could Nintendo have avoided this kind of situation?

The case of the latest version of the firmware (v7.0.0) for the Nintendo console is a special one. It wasn't a software vulnerability, but rather a problem with the console's hardware. What happened in January is that they managed to crack the private keys that that version of the firmware is signed with, in order to be able to modify it. In this case, in order to fix it, the console's hardware needs to be revised, something that Nintendo should already be working on.

On the other hand, in order to avoid software flaws, it is crucial to include security from the very first stages of its design: the so called shift left. Collaboratively integrating security into DevOps workflows, also known as DevSecOps, is an efficient way of preserving the quality and the security of the teamwork, the agility, and the speed of DevOps. These work models have been demonstrably successful compared to traditional models. They allow for the development of higher quality software, which is also more secure, without increasing development times or costs in any significant way.

What would you say are the leading threats to corporate cybersecurity at the moment?

One of the greatest threats is ransomware, especially for small and medium companies that don't have the same level of security as larger organizations. One of the most commonly exploited points of entry for this kind of attack are remote accesses, via Team Viewer, VNC and other similar vectors. In order to mitigate such attacks, organizations must be sure to have robust VPNs that allow them to securely access the organization's resources from outside, with 2FA to ensure that credential theft isn't enough to gain remote access. Another vital step is restrictive network segmentation to contain any incident that could happen.

Another threat that keeps growing is cryptojacking, exploiting the processing power of exposed computers to mine cryptocurrencies. Practices such as threat hunting would allow organizations to actively find these kinds of threats, and would improve their detection and response capabilities.
Threats to critical infrastructures will continue to grow.

This is especially true in the context of industry 4.0 where IT and OT networks are starting to work together, and PLCs and other components of the OT network acquire different transmission capacities to traditional cable-based network. In such complex case studies, it is necessary to create a hostile environment for the adversary. This includes optimal segmentation between OT and IT, avoiding direct exposure of the OT environment to the Internet (including access to vendors), deploying detection and response capabilities on machines that cover both environments, and maximizing the control of privileged accounts.

Finally, one of the threats that we'll keep coming across in organizations and industrial environments is industrial espionage. Even with particularly high levels of security, there are always weak links that could go unnoticed in traditional pen testing processes. For example, one of the most noteworthy examples is the use of video conference systems. They are rarely well protected, and their communications are more often than not unencrypted.

What is the importance of digital forensics in the business world?

Before carrying out any kind of digital forensic analysis, the first thing will be to find out what has happened, what the aim of the analysis is, and what assets have been affected. We won't act in the same way to analyze a Windows network affected by a piece of ransomware as we will to investigate how an invoice has been intercepted in a CEO scam. We need to adapt our methodology on case by case basis. Digital forensic analysis is a basic function in companies in order to answer such questions as: what happened? And, how or why was it possible? And this analysis serves not only to investigate an incident, but also to shed some light in case of disputes, employees that steal information, threats carried out via corporate email, among others.

What is biohacking, and what application could it have for companies?

The term biohacking has a very broad definition, and can refer to several disciplines and movements, from DIY biology, grinders, who alter their bodies to add technology, to nutrigenomics. At Zerolynx, in collaboration with Patricia Rada, doctor of biochemistry at Ciberdem (Center for Network Biomedical Research), we're carrying out research on storing and concealing encrypted information in DNA. It's a complex study in which we're finding barriers that are hard to overcome with the technology that we have available to us nowadays. We've done tests on simulators, and we're now performing real tests on bacterial strains. With appropriate resources, and seeing how interested some organizations are in making sure this moves forwards, we believe that we could see some kind of prototype in a couple of decades. The possibilities are almost limitless, but it is certainly not something we'll see in companies in the short term.

> **“**
>
> **Over the last few years, the cybersecurity world has become hugely professional”**

Spain is becoming an international reference point. Proof of this lies in the large number of cybersecurity events that take place in our country.

What are the 5 most important steps in an effective incident response plan?

Before an incident occurs, we need to be sure to have a business continuity plan and a corresponding contingency plan; we need to have trained our employees beforehand, so that they are able to detect the incident and know how to react properly, according to what has been established at a corporate level.

The first step in a SIRP [Security Incident Response Plan] needs to be detection, and alerting the incident response team. Since the necessary steps for ransomware, a CEO scam, or a fire in the data center aren't the same, the employees who have detected the incident need to facilitate as much information as possible for the response team, so that they can figure out how to react to a specific threat with a quick analysis.

The next step, in order to ensure business continuity, will be to isolate the affected environments, and to collect the corresponding evidence in order to research the origin of the problem and, if necessary, carry out a complete forensic analysis at a later date. This could lead to legal action if malicious actions are detected. In that case, before any action is taken on the affected assets, the company needs to guarantee the corresponding chain of custody, and the cloning and digital signature of the affected assets to ensure the integrity of the information that they contain. The incident will then be scaled, and, if necessary, the corresponding authorities will be notified. Finally, all actions carried out and lessons learned must be cataloged in the interest of improving reactions to subsequent incidents.

How can a company become cyber-resilient?

Companies need to designate a head of IT security (CISO) with the proper training, and provide them with the necessary resources to carry out this job. This person needs a strong team to back them up, which can work on both the regulatory and compliance aspects of cybersecurity, as well as on the more technical and operative aspects. There are many technologies that can be used to protect corporate assets: systems of backups, firewalls, intrusion detection systems, SIEMs, and so on. Nevertheless, without suitable professionals, all of these measures usually become obsolete and poorly parameterized quite rapidly, and stop working as a real barrier to stop the criminals that threaten companies every day. Any business that doesn't have the capacity to have its own high-quality cyber-team needs to contract professional services from specialist companies in the sector. A trusted vendor, with protection that adapts to what the company needs, is an important option for companies that do not have their own security measures ■

> “Without suitable professionals, all of these measures usually become obsolete and poorly parameterized quite rapidly”

José Manuel Díaz-Caneja

AT TIMES IT IS EASIER TO CORRUPT AN EMPLOYEE THAN TO USE CYBERATTACKS TO BRING DOWN A SYSTEM

When it comes to protecting organization's corporate cybersecurity, there are several fronts. Two of them, however, are particularly important: first, monitoring the human factor, which is often the main trigger for cyberattacks or data leaks. The second is applying intelligence to all processes so that advanced cyberdefense isn't reactive, but instead is based on proactive actions. José Manuel Díaz-Caneja knows this all too well. His is an expert in intelligence analysis and professor for the Cyberintelligence Master's program at the Cybersecurity campus of UFV. We spoke to him to find out about the current state of cyberdefense in companies, and the challenges that still lie ahead.

What role does cyberintelligence play in the current cybersecurity landscape?

The term cyberintelligence always shows up when people talk about cybersecurity. Most of the time, it seems to be limited exclusively to technical analysis of cyberthreats, with the aim of using it to improve an organization's cybersecurity. That is, a reactive concept, totally defensive.

If we were to define cyberintelligence as intelligence developed on the basis of information obtained in cyberspace and which helps an organization's decision-making and planning processes, we would see how its field of action would become much wider. In this case, the aim would no longer be just to contribute to the defense of an organization; it would also have a more offensive and more proactive component. This would then make it easier to take advantage of the opportunities offered by cyberspace.

Cyberintelligence needs to facilitate the creation of strategic and predictive cyberthreat alerts based on indicators. The aim is to prevent and stop, or at least mitigate, the associated risks.

Internal threats are one of the main risks faced by organizations. What are the most frequent?

At the moment, the most frequent are accidents, such as sending information to the wrong email address, not spotting phishing attacks, or errors caused by misconfigurations in IT systems. However, intentional actions are becoming more frequent, due, in part, to the fact that it is often easier to corrupt an employee than to carry out sophisticated cyberattacks to bring down a system.

An example of this is SIM swapping. Why waste efforts on social engineering attacks when it is easier to compromise the employee in a phone shop in order to copy customers' private data and make a duplicate of the SIM card? This is also the case when it comes to revealing sensitive company information.

The problem with intentional internal attacks is that organizations are often unaware of how many employees have privileges to access sensitive information.

What measures should organizations implement to prepare themselves to deal with these internal threats? What does business counterintelligence entail exactly?

First of all, the organization must consider several important questions:

- What does our organization need to protect?
- What are our competitors/ adversaries (or foreign government agencies) trying to discover about us and why?
- How are they trying to do this? What capabilities do they have? Are they using a technical approach or are they trying to bribe our employees?
- What can we do, and what are we doing, to reduce their chances of doing it? What legitimate denial and deception tactics could we use to protect our information? What about our patents and R&D ideas?

> “Intentional actions are becoming more frequent, due, in part, to the fact that it is often easier to corrupt an employee than to carry out sophisticated cyberattacks”

If an organization is unable to answer the first two questions clearly and precisely, it will be unable to answer the last two. In this case, it would result in the organization adopting inefficient security measures to protect itself.

To avoid this, organizations must apply a counterintelligence approach. To this end, they need to work on three specific areas: recruitment; training and awareness; and monitoring and supervision. A first, fundamental step, is to recruit the right people, whose profiles adjust to the access privileges they are going to have. Secondly, training them and raising their awareness of security issues is key, not only in things like how to identify a cyberattack, but also in detecting suspicious behavior in their workmates who may be acting strangely. This involves implementing the discreetest possible procedures for employees to be able to report any supposedly unusual activity.

Finally, organizations must implement a monitoring and investigation program to act as a deterrent. This, however, shouldn't focus exclusively on technical aspects; it should also be used to find out as much as possible about people in key positions in the organization. It is important to be aware of the fact that an insider is often not some high-up in the organization, but rather just the opposite. They are people who occupy middle or low level positions and, for different reasons, are unhappy.

We're used to hearing people talk about intelligence processes with regards to government intelligence. What advantages does it have when applied to any other kind of organization?

The aim of intelligence, in the broadest sense, is to reduce uncertainty and generate knowledge, providing appropriate, relevant, and, where possible, predictive, products. This way, they can provide support in decision making processes and in planning. These are processes that require proactivity and anticipation to stop the organization from getting a nasty surprise.

Intelligence isn't about getting it right. Rather, it is about reducing the chances of getting it wrong. This should be transversal throughout the whole organization. It is often the case that the only effect it has is to reorganize internal information exchange and decision-making processes. It is also important to highlight the fact that, in order for it to work, it must involve everyone in the organization.

> **Organizations need to work on three specific areas:**
>
> - Recruitment
> - Training and awareness
> - Monitoring and supervision

What, in your opinion, are the main threats that companies are facing at the moment?

Paraphrasing what the National Security Strategy 2017 says, espionage is one the main threats for many companies. Its aim is to get hold of competitors' information that would help the perpetrator to gain market predominance at a lower cost. If we look at companies whose work is on projects linked to national security, we see that espionage activities can reveal strategic capacities linked, for example, to defending or protecting critical infrastructure.

The year is coming to an end. What cybersecurity trends to you think will mark the coming decade?

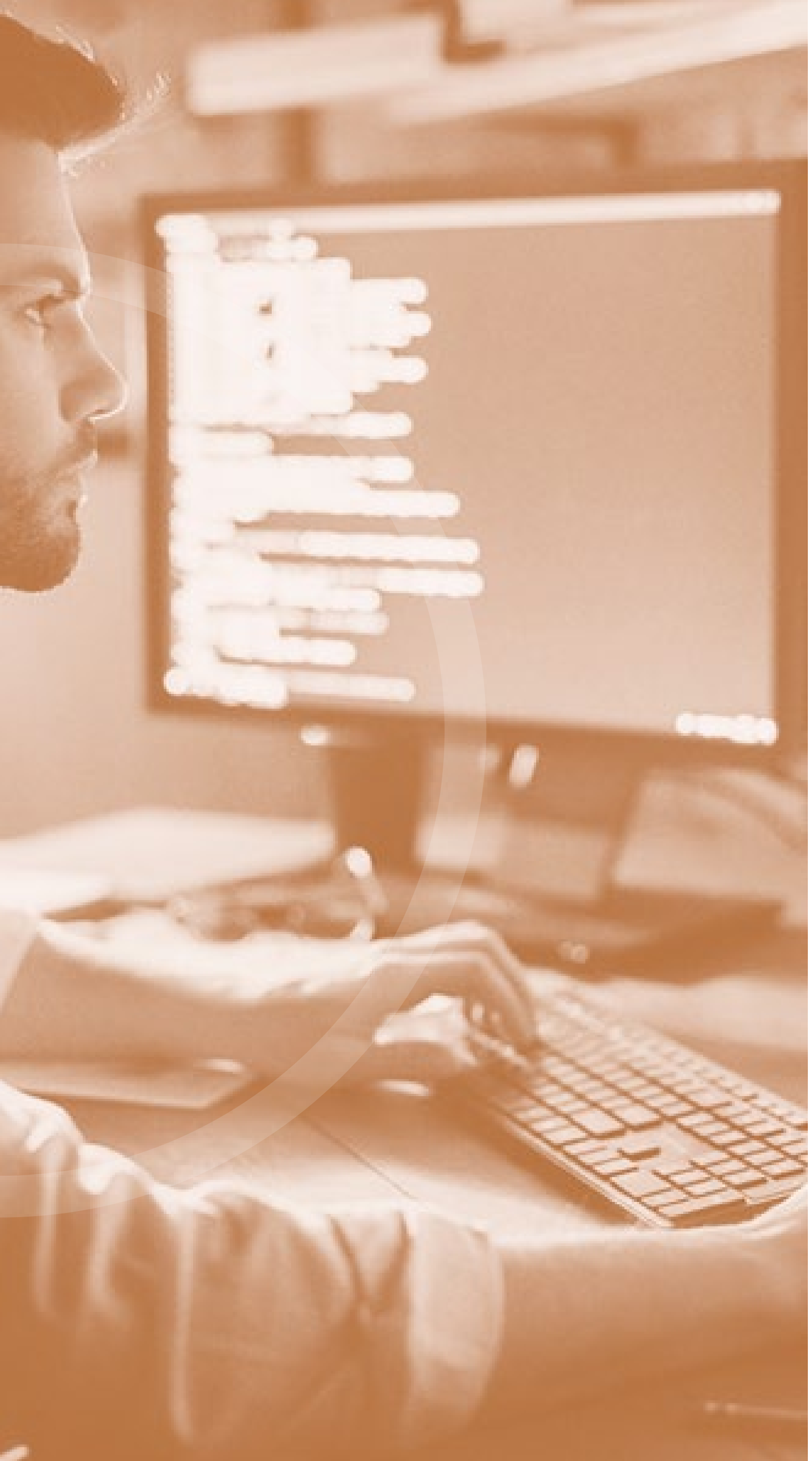
The use of cyberspace to carry out all kinds of activities is here to stay. This means that the trend in cybersecurity will be to keep advancing developments that allow us to protect individuals and organizations in a more efficient way.

However, there's no use in building protective walls based exclusively on hardware and software. History shows that all walls either have back doors or can be breached. This is why we need to provide 360° security. Before this can happen, more imaginative technological proposals need to be added, based on deception, which stop or hinder cyberattacks and, above all, improve early detection alert systems.

All of this involves bearing in mind the fact that, behind every computer, be they attacker or defender, is a person whose aim is often to provoke real-world effects.

This is why linking the identification of cyberthreats exclusively to cyberintelligence isn't realistic. The information we need to be able to attribute a cyberattack cannot be obtained from cyberspace, and we need to get it from other intelligence disciplines ■

> “The use of cyberspace to carry out all kinds of activities is here to stay”



María Campos

WE BELIEVE THAT A COMBINATION OF PRODUCTS AND ADVANCED SERVICES IS ALWAYS NEEDED

This year, we have witnessed the creation of Cytomic, the business unit of Panda Security. Cytomic seeks to respond to the market's current cybersecurity needs, and more specifically, to the most advanced needs of customers in the Enterprise segment, and is a result of the growth of Panda Security.

Cytomic represents the 'cyberatomic' model, which perfectly reflects the company's understanding of cybersecurity. The cyberatomic model, rather than taking the atom as the starting point, goes one step further and focuses on analyzing how these atoms are joined to each other, in order to create something larger, since only through these complex relationships can we understand the process of forming matter.

This is how Cytomic approaches cybersecurity, since, instead of focusing its efforts on different parts, it goes further to gain a global vision. Following this principle, it tries to decipher the relationships between the different events that make up an attack process, it investigates the behaviors that link apparently unrelated events and the behaviors that these events have in common. It focuses on breaking down and defining links made between machines, people, programs and behaviors that lead to an attack. To better understand this, we spoke to María Campos, VP of Cytomic.

What does Cytomic aim to solve?

This new business unit has been created to respond to the most complex cybersecurity needs, to resolve the problem of organizations that have a higher level of cybersecurity maturity. At Panda Security we saw that, despite having an appropriate offering for the mid segment, there was a lack when it came to additional services, platforms to host all the processes required by a key account. These accounts require investigation, incident response, a layer of powerful services, etc. Because of this, we decided to create this new business unit with a combination of products and services, in order to be much more specific, precise, in order to be better adapted and more flexible when dealing with these more advanced cybersecurity needs.

What is the key technological proposal of Cytomic?

Cytomic offers exclusivity, professionalism and specialization, and within its service and solution proposal, these elements translate into effectiveness, simplicity and power. We believe that a combination of 100% cloud-based products and services is always necessary.

In fact, we are pioneers in the development of cloud-native cybersecurity solutions. We provide a response to keep our customers threat-free and to minimize their risk of being exposed. We can thus concentrate this differentiation on three pillars. Prevention, by reducing the attack surface using a zero trust model. Using this model, we catalog applications and don't let any unknown processes, or processes we are unsure about, run until we can investigate them fully. On the other hand, continuous proactive threat investigation; beyond malware and files that may get in through a security breach, we proactively hunt for threats, getting ahead of everything that could happen.

Finally, we provide security tools and platforms to make customers much more effective and efficient by strengthening their security posture. Because of this, we end up with a highly consistent model that, thanks to all the technologies that we apply in the cloud, based on Security Data Analytics, artificial intelligence, on a community model, learning, intelligence sharing... We can thus prevent and detect attacks, as well as providing hunting and remediation services.

Panda Security is a channel company. What relationship does Cytomic have with the distribution channel?

Cytomic was born with a 100% channel philosophy because we need partners more than ever. When we talk about this advanced product-service binomial, we believe that, as a manufacturer, and thanks to the expertise of our laboratory, we can provide the first level of a horizontal service based on cataloging all applications, with a threat hunting service.

We also use the intelligence accumulated over Panda's many years of experience, where we store 365 days of historical data to cover that detection window that, these days, is over 100 days. But we need our specialized parters since, at the end of the day, they're the ones who know the customer's processes, their workflows, the business... And how to apply this technology to the customer's reality. A clear example is threat hunting: we carry out a highly horizontal first level, where, thanks to intelligence sharing, we are able to know what is going on anywhere in the world, all in real time. But it's the partner that is going to know if we're dealing with anomalous behavior, whether someone accessing a database at 3 in the morning is normal for the customer.

Then this specialized service must be provided by the partner. For us, therefore, partners, understood to be partners for services that are truly specialized in applying technology, are key for Cytomic ■

> **Cytomic offers exclusivity, professionalism and specialization, these elements translate into effectiveness, simplicity and power.**

More Information

https://www.pandasecurity.com/business/

Email:

communication@pandasecurity.com