

2018 IN CY BER SECU RITY

THE EXPERTS TALK

INDEX

01

You shouldn't invest in security just for compliance

+ Zane Lackey

02

In the US, cybersecurity is a national priority

+ Soledad Antelada

03

90% of success in the fight against cybercrime is prevention and awareness

+ Silvia Barrera

04

The challenge for cybersecurity in the future won't be malware

+ Pedro Uría

05

There are companies spending vast sums on security that could still have poor protection

+ José Sancho

06

Cooperation between the public and private sectors is essential to combat cyberthreats

+ Javier Candau

07

The key to resilience is having a mature strategy and a good partner

+ Nicola Esposito

08

WannaCry marked a before and after for Spanish companies

+ Mónica Valle

09

Cryptojacking is one of the most brilliant attacks I've seen

+ Xavier Mertens

10

Cybersecurity isn't negotiable: the loss of resources can mean the end of your company

+ Enrique Ávila

11

There's no such thing as 100% security

+ Pablo González

12

The European cybersecurity Hub

+ Panda security summit 2018

PRO LO GUE

As humans, one of the most basic necessities that we have is security. From birth, we need “security” in every different aspect of our lives, and it is something that becomes a trait that follows us, forming part of our very nature.

This security is something we extend to every aspect of our daily lives, including protection for the technological systems that we use.

Throughout the 28 years of Panda Security’s history, we have been able to analyze the evolution of the IT

security world, witnessing and participating in the breakthroughs that have changed the world.

The continuous progress of technologies has caused those responsible for threats to make their attacks and the tools they use more sophisticated.

Cyberspace is increasingly hostile, forcing organizations to have the most innovative technical means to face up to these attacks and their possible effects, as well as to adopt proactive security policies to mitigate them. These days, cybersecurity

goes beyond protecting the information stored on our systems; it also aims to protect the technological infrastructure that supports this information, and which makes us work as a society.

The best thing about working in the field of IT security is meeting outstanding professionals from the sector with whom we can share concerns, experiences, and points of view, such as those collected in this section called “2018 in Cybersecurity, The experts Talk”.

Marta Zapata

Global Communication Manager
Panda Security



Zane Lackey

YOU SHOULDN'T INVEST IN SECURITY JUST FOR COMPLIANCE

The concept of the cybersecurity manager is evolving, as the role shifts from the traditional “gatekeeper” to a more universal, company-wide security facilitator.

Zane Lackey, is one of the most important white hat hackers in the world, and author of books such as Mobile Application Security and Hacking Exposed: Web 2.0. Currently, Lackey is the co-founder and CSO of Signal Sciences, a web application

protection platform, and is also a member of the Advisory Board of the Internet Bug Bounty Program and the Open Technology Fund.

Although new infrastructures, services, and applications are being created, such simple things as security failures at the endpoint or a lack of two-factor authentication systems continue to be the cause of the global attacks making headlines.

[Discover More](#)

Panda Security:

What techniques do you use to detect a vulnerability and expose a threat to avoid an attack?

Going back to my pentesting days, which was quite a while ago at this point, the most common things I would look for were the assumptions made in the design of the system. Then I would look for ways those assumptions might be violated. On the defensive side, I took that mindset thinking about how to empower development teams and DevOps teams. That was one of the biggest lessons learned for me — going from a white hat, security consulting, pentesting kind of thing over to becoming a CISO and building a security organization, is really focused on how to give the engineering team as much visibility into what's going on in production as possible.

PS: How do programs like Internet Bug Bounty help to resolve vulnerabilities that have been discovered? After a flaw is discovered, how do you act?

I know there have been some changes in the Bug Bounty program recently, so I don't want to say anything that would be incorrect there, but I think that from having run multiple Bug Bounties in the past, the important thing is trying to establish good communication with the researchers that come in. Because a lot of times, you'll get a report that is partial or doesn't contain all the info that is needed to reproduce the issue. So being able to say, "Hey, these are the five bits of information that we need so we can take this to the relevant service team or application team", can help communication on both sides. And at the same time, trying to communicate back to the researchers so it's not just a black box for them. Trying to be as transparent as

possible on both sides — that's what really leads to a good Bug Bounty experience, both for the researchers and for the organizations that actually work with them.

I think anyone who's run a Bug Bounty program gets used to seeing all kinds of things. You see everything from systems that you didn't know about, to pretty much every type of vulnerability, even ones that you don't think that you have. So I really strongly believe in the value of these programs, and I think they complement pentesting very well. Combining the two can really help most security programs out there. The reason I like Bug Bounty programs so much in combination with pentests is because it allows you to focus your pentests on very specific areas rather than trying to have them test everything when they don't have time for that. So you can use your bug bounties to try and get very wide coverage, and you can use your pentests to try and get very focused and specific coverage.

**“USE YOUR
PENTESTS TO
TRY AND GET
VERY FOCUSED
AND SPECIFIC
COVERAGE”**

PS: The NHS has recently hired white hat hackers to identify cyberthreats. Do you believe ethical hackers are indispensable in today's organizations to avoid breaches and strengthen defense?

For every organization, you need to be thinking about how people actually attack your systems. So white hat hackers, and pentesting, and bug bounties, those are all a piece of it. They're not the full story, but they're a piece of it. You don't want to be doing security just for compliance, or just trying to check the box of different defenses to put in place. I challenge folks to have the number one thing that they're thinking about as they're trying to build a security program be: how would an attacker actually attack my organization?

And really use that to drive the defensive programs that you put in place. And that's where red teaming, white hat hackers, bug bounties, and all these ways to test your system can be a very powerful feedback

loop. Because they can show, when your systems are being attacked, "this is where they went." And that can focus your defenses.

So I really strongly believe in balancing offense and defense and using one to guide the other, and not just trying to do one in isolation.

PS: How can you implement DevOps to make companies safer?

I truly believe that embracing DevOps and embracing Cloud can make you safer. The reason for that is, in any development methodology, you're still going to have vulnerabilities. So as soon as you recognize that fact, the logical conclusion is that the development technology that will allow you to react the fastest is the one that can make you safest. In the old model of waterfall and changing applications very slowly, the problem was there was no way to react quickly. So this is why DevOps, Cloud, and the shift to Agility can actually make us safer.

PS: What can we learn from massive data breaches like Equifax, which happened via a web application vulnerability?

I'd say there are two things to learn from the breaches that we see every day. One is that, 99% of the time, they are the completely common, off-the-shelf things — its things that weren't patched, it's a weak password, its malware on an endpoint, etc. So going back to a previous comment, I would encourage all organizations to not think about the "insane, state-sponsored zero-day that's crazy complex", but rather to focus on the basics: how do you get coverage over malware on your endpoints? How do you get two-factor authentication on all your accounts? And how do you get coverage over the web application layer?

Because I think the other lesson that we're all just starting to see in terms of the breaches but which we've been seeing in the trenches the last few years, is that historically the security risk was at the infrastructure layer and the network layer, so

"I TRULY BELIEVE THAT EMBRACING DEVOPS AND EMBRACING CLOUD CAN MAKE YOU SAFER"

we always thought firewalls and IDSs and things like that could mitigate it. But over the last several years the risk has all moved up to the application layer and out to the endpoint. So learning where your risk actually sits is the number one lesson we should be learning as an industry right now, across the breaches that we've been seeing.

PS: Do you think companies will be ready for the GDPR? What will they need to do to be compliant and protect their data?

With any new compliance regime, there's a lot of concern with it up front because no one is exactly certain what it looks like yet. So I think it will be a little fuzzy at first, then you'll see products and services emerge to help with it and you'll see a much clearer picture of what the auditors are actually looking for and what steps really need to be taken as part of that.

Security and compliance are two separate things that sometimes overlap in small

pieces. So defending your data, and not just being compliant with something, you have to ask: how do I defend my endpoints? How do I defend my web applications and my APIs and other things at the application layer? Because those two buckets are where so much of my risk is. So you should focus on getting visibility into those, getting effective controls into place around malware on the endpoints, two factor authentication for as many services as you can put it on, and then getting coverage and visibility and protection for your application layer.

PS: In terms of application security, do you prefer security by programming from within, or do you prefer protecting it from the outside?

The answer is both. For defending applications, how you do that effectively is you think about how to eliminate as many bugs as possible during the development cycle, but at the same time you recognize that there will always be vulnerabilities. So you couple

that up with getting visibility and defense into the code that's actually in production, and not just try to scan for bugs once it goes out and then just ignoring it once it's out there live on the Internet. I think that's been a major failing of the SDLC for the past 10 plus years.

The biggest piece of commonality I see amongst organizations that are doing this well is that they try to eliminate bugs before production. they recognize that there will always be vulnerabilities, so they are really investing very heavily in getting visibility into how those services are being attacked in production and using that to bring that visibility directly to the development teams and the DevOps teams themselves, so that they can self serve with that information and not have to rely on the security teams to defend the services that they're building.■

“SECURITY AND COMPLIANCE ARE TWO SEPARATE THINGS THAT SOMETIMES OVERLAP IN SMALL PIECES”



Soledad Antelada

IN THE US, CYBERSECURITY IS A NATIONAL PRIORITY

Despite new intrusion methods and the spread of attacks, for Soledad Antelada, what's really changed in cybersecurity is people's awareness and how the media treats the topic. Systems Engineer at the cybersecurity department at the Lawrence Berkeley National Laboratory and an expert in the sector, she believes that cybersecurity has evolved from a small underground movement to entering the collective consciousness to become a global phenomenon. Soledad Antelada, one of the most influential Hispanic women in the technology world, has a

key task: guaranteeing security of a system in which thousands of people work.

The Berkeley Lab is a prestigious scientific research center which has produced 12 Nobel Prize winners. It is a United States national laboratory managed by the University of California. The department of cybersecurity is in charge of protecting the laboratory and the entire network of institutions dependent on the US Department of Energy.

An expert in cybersecurity, she tells us what the keys are to protecting these kinds of institutions.

[Discover More](#)

Pentesting to stay ahead of cybercriminals

Soledad works as an external agent, that's to say, she pretends to be an attacker to penetrate a network to get into a system and jump from one network to another. "I always act as an intruder", she adds. To do this, she uses scanning and exploit tools or develops her own. Among her favorites are Python, SSH Brute Force, Nessus for scanning systems, and Burp and Netsparker for scanning web applications. To exploit, she uses "a lot of manual scanning or metasploit and SQL injection"

Antelada stresses the importance of penetration testing at Berkeley Lab: "This type of tool is a priority for us. We want to find out about vulnerabilities first and take care of them, before attackers discover them" She also says that at the Department of Energy, cybersecurity audits are performed to evaluate the security of the lab.

According to Soledad, "during the audit period, they evaluate the general vulnerability of the lab. If they don't find anything, then we are doing our job".

"Patience is the best virtue in pentesting", she adds. "It takes a lot of trial and error to discover on your shift what the bad guys are trying to do 24/7. And then have to fix it to boot."

Tips for security professionals in a connected world
Soledad thinks the sector has to "invest more in highly qualified people than in teams".

By supporting experts and strengthening cybersecurity departments, both companies and public institutions can stay ahead of the curve and don't have to wait for an attack to defend themselves. Antelada adds that, in the US, greater importance is given to the sector.

"Regardless of the government in power, cybersecurity is a priority for the entire country."

For Soledad, employee education is also a priority. According to her, this will become more important as the Internet of Things grows. She explains the case at Berkeley Lab: "There we've got all kinds of instruments connected to the network, such as lasers and microscopes, which are also attack vectors."

If the security of these devices is compromised, "the scientists that use this equipment need to be contacted and shown how to fix the vulnerability." It's not just about fixing the problem, but educating users about the vulnerability, how they found it, and how to fix it. This, says Soledad, "helps users adopt the right mindset regarding cybersecurity and from then on they can be on the lookout for suspicious behavior."

Also, to protect institutions, cooperation of different areas in an organization is fundamental. "There should

**"REGARDLESS
OF THE
GOVERNMENT
IN POWER,
CYBERSECURITY
IS A PRIORITY
FOR THE ENTIRE
COUNTRY"**

be real support between employees of the departments. Among those in charge of storing and managing data, system managers, software developers, etc., all should be connected with the cybersecurity department because they cannot work on their own, they depend on the administrators to protect them.”

Women in the cybersecurity sector

At Girls Can Hack, Soledad tries to get women interested in technology to encourage them to get involved in what has traditionally been a masculine sector. “I’m the first and only woman at the Berkeley Lab cybersecurity department, says Antelada, “and even though the number of women at companies is still very low, I’ve seen a change and women are now beginning to take an

interest in the field.”

To change this, what does Soledad suggest that to women who want to get involved in the sector? “Just do it. It’s a very dynamic field that needs a lot of people and diversity. Cybersecurity departments are monotonous, which is a flaw. Security problems are diverse, and the more varied the departments are, the easier and more creative the solutions will be. ■

**“JUST DO IT.
IT’S A VERY
DYNAMIC FIELD
THAT NEEDS
A LOT OF
PEOPLE AND
DIVERSITY”**





Silvia Barrera

90% OF SUCCESS IN THE FIGHT AGAINST CYBERCRIME IS PREVENTION AND AWARENESS

A renowned cybersecurity expert and writer, Silvia was the head of social media investigations at the Spanish National Police Corps for 5 years, and headed the digital forensics group of the National Police's Technology Research Unit for another 3 years.

We had the opportunity to sit with her now that she has quit her job at the Police Force, and talk about how the cybersecurity landscape has changed, and the ways in which companies and public institutions can defend themselves and combat cybercrime.

[Discover More](#)

PS: How do you feel about this new stage in your life?

I feel like a whole new world of possibilities is opening up before me. The Police Force has given me exceptional vision, knowledge and experiences that I couldn't have had anywhere else. It's been a privilege. Nevertheless, until now, as a member of the Police Force, my job has always had a reactive nature, identifying and arresting the 'alleged' bad guys. However, the paradigm of the fight against cybercrime has changed. Today, less than 4 percent of cybercriminals are identified (let alone sentenced), but at the same time we also know that the great majority of Internet crimes (up to 80 percent) could have been prevented.

Cybercrime is a very profitable business model, with little exposure for the perpetrator and very difficult to fight. It's unavoidable and is definitely on the rise. The reactive approach to fighting it is necessary but not very effective or sufficient (because of the very way the Internet works).

In this context, it is important to be aware that 90% of success in the fight against cybercrime is prevention, awareness and security controls, and 10% is reaction (investigation and prosecution). We must act with all human and technical resources available to us in order to prevent cybercrime and, should it occur, be ready to react quickly and decisively. And that is where the concept of resilience comes to play.

PS: Why do you think an event such as the Panda Security Summit is necessary?

Events like this are necessary to give visibility to cybersecurity, explain some of its key concepts and give it the central place it must occupy.

In the corporate world, all business activities rely on computer data and IT structures. And, at public level, crime always has technological implications relative to its modus operandi or in order to obtain the necessary evidence to investigate it, and let's not forget that a country's national

security can be seriously compromised by cyberthreats.

PS: In your opinion, what level of cybersecurity awareness and training is there in Europe?

I've been a member of different cybercrime and cybersecurity working groups in Europe for four years and have participated in dozens of meetings.

That's where you see the difference in resources and the importance given to cybersecurity by each country. Spain is ten years behind countries such as the Netherlands, Germany or the United Kingdom for example, where the public sector dedicates many more human and technical resources to cybersecurity. Even at legislative level, there are countries such as Germany that have specific IT security laws.

“CYBERCRIME IS A VERY PROFITABLE BUSINESS MODEL, WITH LITTLE EXPOSURE FOR THE PERPETRATOR AND VERY DIFFICULT TO FIGHT”

PS: In your opinion, how prepared are Spanish and European institutions to combat cybercrime?

Spain has no reason to envy other European countries. Actually, we have demonstrated to be very efficient in the fight against cybercrime. It's not a question of lacking competence, as it is a lack of human and technical resources, and cybercrime and the digital world require significant investments.

During a police exchange I had with Germany's Federal Police for the investigation of a case affecting a number of German banks, I could see how they set up a global team of police officers, prosecutors and members of the privacy sector to work exclusively on that case until it was solved or the investigation came to an end. In Spain, police investigators usually work on dozens of cases at the same time, and despite there is contact with people from different areas, there is not so much teamwork.

PS: What do you feel is the greatest problem today regarding the security of companies and institutions?

First the human factor and then the technical side. In technical aspects, the problem can be avoided by properly evaluating risks and using internal and external checks and controls. You can't just think about the employee; organizations and companies need to integrate and align cybersecurity as a strategic objective of the business and as such assume the costs of IT security. There will be difficult times ahead in terms of security risks and data protection, and there will be stiff penalties and consequences, particularly in terms of corporate reputation, as illustrated by the recent cases of Facebook and Tesla.

PS: What challenges do you think businesses and organizations will face with respect to IT security in the next two years?

The change in consumer mentality. We have to try to be as preventive as possible, acting at every point of the process to mitigate the cost of cybercrime for users, but we cannot truthfully tell users or customers that they will never be the victim of an attack. They will be, and consequently they must be prepared.

The more concerned you are about your cybersecurity, the more secure you will be, and this goes for your business, reputation, etc. Cybersecurity never costs more than the damage that can be inflicted. The Internet offers an infinite array of tools and features that can make life easier, but it can also ruin it.

“THERE WILL BE DIFFICULT TIMES AHEAD IN TERMS OF SECURITY RISKS AND DATA PROTECTION”

PS: What does it mean for you that a company or institution is resilient from the point of view of cybersecurity?

Resilience is the best factor for gauging the strength of a company or institution. It tests how you manage communications, data, security and IT infrastructure. The capacity to recover from a possible attack is also a factor to evaluate your readiness and how you can improve it. Ultimately, it shows who can successfully adapt to technological changes and

demands. And with regard to external customers, how you take care of this within your organization will also reflect how you take care of your customers' information. Your reputation and their trust is at stake.

PS: In your view, what aspect of resilience is the most important to keep companies and institutions secure?

All of them. From prevention, avoiding the vast majority of attacks and incidents, to detection and response.

Although there is no 100 percent security, as we know, almost 99 percent of attacks can be avoided. How? By taking into account all factors of resilience. It is important to be aware that cybersecurity is like taking care of your own security and personal health. You might not get a tangible return from it, but it guarantees a long life, full of satisfaction and success. That is resilience. ■

“THE CAPACITY TO RECOVER FROM A POSSIBLE ATTACK IS ALSO A FACTOR TO EVALUATE YOUR READINESS AND HOW YOU CAN IMPROVE IT”





Pedro Uría

THE CHALLENGE FOR CYBERSECURITY IN THE FUTURE WON'T BE MALWARE

The director of the laboratory PandaLabs, Pedro Uría, put forth the keys for business security, protection and resilience, now that malware is no longer the problem.

Instead, hackers are the future challenge of cybersecurity, as they use more complex methods. “New attacks, like those that don’t use malware, are the target of threat hunting services

[Discover More](#)

PS: What's the biggest challenge facing organizations and companies with respect to computer security today?

The biggest challenge is to make them aware that the security of their IT assets is critical and that they face a constant risk of attack. According to the INCIBE, Spain witnessed a record number of cyberattacks in 2017 with more than 120,000 incidents, a 140 percent increase in just two years. The forecast is for this figure to rise in 2018, and with more complex attacks.

PS: What can we learn from security breaches based on vulnerabilities, such as Equifax?

That no organization is safe from cybercriminals. The use of vulnerabilities to infiltrate a company's systems is a common technique. This case is the largest leak of personal information data ever known. Hackers stole the data of 147.9 million Americans.

Zero-day vulnerabilities are traded on the Deep Web and

are a highly successful vector of silent attacks for criminal organizations. For example, Microsoft has just released an urgent patch for this type of critical vulnerability in the Windows Defender antivirus on Windows 10. As you can see, not even organizations such as Microsoft are secure on such critical issues as its antivirus.

PS: Malwareless attacks and attacks without files are new trends, how can organizations and governments combat them?

The challenge for the future of cybersecurity lies not in malware, but in hackers. They are expert, highly-trained cybercriminals with resources, capable of compromising a system in an organization without being detected as they don't use malware or files that could give them away.

To combat them, companies have to protect each and every one of their IT systems with an advanced cybersecurity solution able to constantly monitor in real time what happens on every computer.

They must also be able to ascertain whether actions taken are genuinely legitimate, even though they are performed with legitimate applications or without malware.

PS: How can we achieve resilience in the face of malware attempts to evade the scanning of security solutions?

To achieve cyber-resilience, all of the organization's IT resources must be protected with an advanced security solution capable of detecting, preventing and remedying attacks. Similarly, the solution has to monitor in real time all processes and actions taken by users locally on the physical computer. This requires the monitoring, supervision and attestation of all processes and actions by a specialized team of experts, like the PandaLabs team.

It is also important to educate managers, workers and contractors to prevent them from being tricked into becoming an unwitting vector for attacks.

“NOT EVEN ORGANIZATIONS SUCH AS MICROSOFT ARE SECURE ON SUCH CRITICAL ISSUES AS ITS ANTIVIRUS”

PS: We talk about keeping organizations secure, protected and resilient when malware is no longer a problem. Have we already reached that level of protection or is malware still the main problem for companies?

It depends to a large extent on how mature a company is in terms of the importance given to cybersecurity, and the advanced protection solution it uses to protect its infrastructure.

For Panda Security, malware is no longer a problem thanks to the high visibility we have with our advanced solution, Panda Adaptive Defense and the model for classifying 100 percent of the processes that run on the endpoints we are monitoring. Thanks to this, we are able to anticipate attacks and protect the systems of the companies that place their trust in us.

Similarly, the Threat Hunting service, delivered through the Panda Adaptive Defense platform, is focused on discovering new threats, including malwareless attacks.

For other companies, malware continues to represent a big problem. Every day there is more malware, the number of incidents is greater and the trend for 2018 is set to see an increase in the volume and complexity of attacks. ■

“FOR PANDA SECURITY, MALWARE IS NO LONGER A PROBLEM”





José Sancho

THERE ARE COMPANIES SPENDING VAST SUMS ON SECURITY THAT COULD STILL HAVE POOR PROTECTION

The so-called virtual world, cyberspace, is where practically all our professional lives along with many personal activities take place, and it is also where attacks occur.

The main question then is why are we attacked in cyberspace? The prime motive is purely and simply financial, and the essential source of financial gain in this context is the information we have: the data. So why attack in this environment? The virtual world is software-based and software is vulnerable.

Cyberattacks are quick and relatively cheap compared to attacks in the real, physical world. This combines with the fact that existing laws against cybercrime are ineffective.

Such laws are evolving gradually, though the problem of attributing responsibility persists as, if the culprit cannot be identified, if there is no evidence left, it is as if there is no crime. And as we all know, in cyberspace it is relatively simple for a well-prepared criminal network to leave no trace.

[Discover More](#)

The second element to consider is businesses. More companies than ever have core businesses that are service-based, and this translates into a huge number of bits of information, a very attractive target for cybercriminals.

Finally, governments will become a crucial element in the near future in terms of security. It is not by chance that in the United States, China or Russia there are technology companies that cover all layers of our digital activity, since these make up the backbone of today's economy. In this scenario, Europe is lagging behind. Similarly, we are witnessing how a new cyberwar is being waged, and is probably the only war able to transfer wealth from one state to another. The states are main players in this war: they have the means, the motives, and the opportunity.

It is evident that in the coming months, these developments in cybercrime will come thick and fast. Attacks will go further because the people behind them are learning rapidly and

the tools available to them are also more sophisticated. All the players involved in security in one way or another need to bear in mind that the preventive measures we have taken so far, based on detecting an attack as quickly as possible, are not infallible and take too long in a mobile and aggressive environment developing faster than our defenses.

The cybersecurity triangle

At Panda we take a holistic view of advanced cybersecurity. This view can be framed as a triangle around which we work to ensure security, with the following vertices:


People Programs Data

The attack surface has grown exponentially. The transformation to a digital society involves more and more software and more data, and as there are an infinite amount of vulnerable points, complete protection by means of product is now impossible. Such security requires additional people to validate and examine what the products are not able to detect or to arbitrate when two products offer different diagnoses.

So, security for us consists of collecting all the relevant data concerning the behavior of a program, run by a person. This vision clashes directly with the more traditional perspective of using barriers to prevent cyberattacks.

“IN THE COMING MONTHS, THESE DEVELOPMENTS IN CYBERCRIME WILL COME THICK AND FAST”

The truth is that today all barriers can be penetrated because software is vulnerable. There is no balance between the investment made in security and the probability of an attack and its impact. So there are companies spending vast sums on security that could still have poor protection. This is because the investment is not really focused on securing the devices that contain the valuable assets that need protection: the endpoints. ■



**“THERE IS NO
BALANCE BETWEEN
THE INVESTMENT MADE
IN SECURITY AND
THE PROBABILITY OF
AN ATTACK AND ITS
IMPACT”**



Javier Candau

COOPERATION BETWEEN THE PUBLIC AND PRIVATE SECTORS IS ESSENTIAL TO COMBAT CYBERTHREATS

Javier Candau is the head of Spain's National Cryptologic Center (CCN-CERT), he will be offering his view of the cybersecurity challenge in Spain.

All security dimensions are important for a company, according to Candau, but the

confidentiality of certain issues and processes is particularly relevant. According to him, management has to understand that a business is sustained by its systems and the information it generates, so this is a strategic decision, as are vigilance and auditing.

[Discover More](#)

As the head of the CCN-CERT, Javier Candau knows what the keys are for a government in the fight against cyberthreats. These include the implementation of improvements in areas such as detection capabilities, considering cybersecurity as a horizontal service; collaboration between the public and private sectors; the response, which has to be rapid and round-the-clock across all points of the corporate network; and deterrence.

So far, sectors such as the aeronautical industry, the general public, and the defense or energy sectors have been the main targets of complex attacks.

In order to face these types of incidents, the CCN-CERT is looking to advance awareness among government authorities and business management. It also aims to improve the capacity to detect complex attacks with anomaly detection tools such as CARMEN, which must integrate with tools for correlating the logs of organizations and, essentially,

with endpoint tools. Candau also highlights the work being done to improve the cybersecurity structures of organizations, aiming for some services to be provided horizontally and for technical staff to be adequately qualified through training programs and the provision of technical information on technologies and configurations.

Cooperation with the private sector and challenges in 2018

Large companies are working with the Government to be able to deal with cyberattacks. However, first it is necessary to establish confidence in each party, explains Candau. Then they can work towards complementing and reinforcing the security services that the private sector provides them. In this way, the head of the CCN-CERT hopes that companies will at some point share information about the attacks they suffer and their cybersecurity concerns.

The essential cybersecurity challenge for the government this year is to provide much

more proactive horizontal services, with the setting up of the Security Operations Center of the Spanish Central Administration. In addition, Candau explains that the Center is working on improving exchange platforms, detection capabilities, auditing capabilities, and training platforms and content.

CCN-CERT's approach to combating cybercrime against the state culminates with the identification of the origin of the attacker. To this end, and in line with current regulations, the government organization operates in terms of risk/impact and speed of response.

Javier Candau admits that cybercrime has very different complexities. These range from botnets, which are generally easy to detect and disinfect, to organized crime attacks that look for direct financial benefit or the theft of information, passing through complex ransomware of difficult cryptologic analysis.

The head of the CCN-CERT also underlines that the targets

set are sufficient to protect the country's critical infrastructure against cyberattacks, but these systems do not undertake the challenge of protecting operational networks. Candau recognizes that it is no longer acceptable for these not to be interconnected, as businesses need this information, so he advocates coherent security policies and thorough vigilance of interconnections as well as traffic and anomalies in industrial protocols. Security must therefore be applied in all dimensions: physical, cyber and human. ■

**“THE WORK
BEING DONE TO
IMPROVE THE
CYBERSECURITY
STRUCTURES OF
ORGANIZATIONS”**



Nicola Esposito

THE KEY TO RESILIENCE IS HAVING A MATURE STRATEGY AND A GOOD PARTNER

Nicola Esposito, Director of Deloitte's CyberSOC EMEA Center and Partner at Deloitte Advisory, will explain how Deloitte, from its Cyber Risk area, helps organizations to strengthen their

risk and security management program. In advance of the summit, we asked this expert about resilience in the corporate cybersecurity environment.

[Discover More](#)

PS: What are the most significant advanced threats facing companies today?

Advanced threats combine numerous tools, techniques and targeting methods. Malware is currently one of the major threats due to its capacity to spread rapidly across an organization and even around the world.

PS: Which aspect of resilience would you say is most important for the security of companies?

You can't single out one aspect. All of them (prevention, detection, containment, response and continuous improvement) have to be taken into account to adopt a serious approach to IT security. In line with this approach, and in order to offer its customers an end-to-end solution, Deloitte has developed its Common Storefront based on the four areas of Strategy, Security, Vigilance and Resilience.

PS: How can the creation of an integrated and connected ecosystem contribute to improving corporate security infrastructure?

The creation of this ecosystem can help make companies more secure and become part of a chain of security. This is one of the reasons why Deloitte promotes the Threat Intelligence network, so as to share indicators of compromise (IoCs) and increase the detection capacity of customers. Such networks allow these IoCs to be shared practically in real time, and consequently reduce the time of exposure to the corresponding malware.

PS: What risks do non-resilient companies face?

Non-resilient companies are probably not taking cybersecurity risks seriously. This is the biggest

challenge. Once a company's management recognizes the threat, it needs a trusted partner to set up a robust security program. So the second challenge is to find a partner able to guide you along a potentially complicated path.

PS: What are the keys to creating resilient companies?

The key to resilience is having a mature strategy and a good partner. With a mature strategy you can address risks in the proper way, starting with business risks and not focusing on them directly from the technological perspective. This strategy should include the values mentioned earlier: Security, Vigilance and Resilience. It is also important to have partners with a global vision, who understand the scope of current threats, and have end-to-end capabilities to understand business risks, advise customers accordingly, and implement and operate the technologies to make their business resilient.

“THE SECOND CHALLENGE IS TO FIND A PARTNER ABLE TO GUIDE YOU ALONG A POTENTIALLY COMPLICATED PATH”

PS: What is the risk of ignoring resilience?

The greatest risk is the likelihood of being hit by a cyberattack and the inability to recover from it. It is not just that critical systems are compromised, there is also the potential damage to brand reputation, which in some cases may take years to restore. There are also risks associated with regulatory compliance, which are related to the security controls implemented in every company.

PS: To what aspect of cyber-resilience should we pay most attention?

The aspect of resilience that is often ignored, or not adequately considered, is detection. Mainly because detection means having visibility, and to have this, you have to understand where and how to pay due attention to all the other sections that comprise cyber-resilience.

At Panda we know that detection and the response to attacks is essential to business cybersecurity. That's why tools such as Panda Adaptive Defense guarantee the protection of aspects that could sometimes be overlooked. ■

**“DETECTION
MEANS HAVING
VISIBILITY”**





Mónica Valle

WANNACRY MARKED A BEFORE AND AFTER FOR SPANISH COMPANIES

She is a journalist with many years' expertise in cybersecurity matters, and she now also has a new book.

Mónica Valle has just launched "Ciberseguridad, consejos para tener vidas digitales más seguras"

['Cybersecurity, Tips For a More Secure Digital Life'], which is aimed at the average Internet user, although she herself has been involved with several of the world's most important cybersecurity companies for years.

[Discover More](#)

With such an extensive background, Valle is more than qualified to paint a picture of the current cybersecurity situation in Spanish companies. A situation in which, she believes, “WannaCry marked a before and after in terms of awareness. Large companies are already up to speed, because they’ve been dealing with this for a long time, and they already see it more as an investment, rather than an expense.”

In cases like this, “the problem lies with small and medium sized companies; for them, this does actually mean finding extra money in the budget, something that isn’t always easy to do.” These companies have had the most catching up to do, and more still since the adoption of the GDPR, something that caught many of them off guard.”

Pending tasks for cybersecurity

For her, “there’s still a lot to be done” when it comes to corporate cybersecurity. Namely, “a lot of the time,

people are reactive: nothing is done until something happens in another company. But in cybersecurity, this is a mistake; you need to be preventative and proactive, putting measures in place before something happens. With ransomware attacks, for example, when you get attacked, the damage is already done, and it’s going to be very difficult to recover anything; companies need to be aware of this.”

“It’s very important to know how to react,” she affirms, “Because once you know how to react, you can minimize the damage. Companies that still aren’t aware of how important prevention is in cybersecurity are also unaware of how important it is to react properly, or how important it is to ensure that any damage is kept to the minimum possible.

The fact remains, “those who want to attack you have countless options, and can do so from many sides, which isn’t easy to prevent. All the experts say the same: every company has been or will be attacked.

This is why it’s vital to focus both on prevention and on knowing how to react.”

On the other hand, there’s a factor that makes protecting a company’s cybersecurity even more important: “These days, companies don’t just have to protect their information; they also have to prove that they comply with some basic cybersecurity rules. And what’s more, if they break the law, the fines are so much higher.”

Any company can be attacked

However, “there are companies that think they’re not ‘important’ enough to be attacked; but, isn’t your information important to you? Without that information you’re nobody, and you wouldn’t be the first company to have to close down as a result of losing this information. Whatever size company you are, any information that you hold is very important – at the very least, for you.”

Likewise, “it’s also important to bear in mind the reputational damage that an attack can

**“YOU NEED TO BE
PREVENTATIVE
AND PROACTIVE,
PUTTING
MEASURES IN
PLACE BEFORE
SOMETHING
HAPPENS”**

cause. Cybersecurity is based on the trust of your clients, your providers, etc., so reputational damage is among the biggest risks for any kind of company.”

The key: employee training

Whenever we talk about cybersecurity, the same question always pops up: do companies that care about cybersecurity do so because of their own convictions, or because they're scared and they fear what could happen to them? To what extent do awareness of the subject and concerns about the consequences of a cyberattack actually influence one another?

Mónica Valle has no doubts about her answer: “Many, it's true, are scared. As there isn't really much of a cybersecurity culture, many companies get scared because they don't know about these subjects. But when they learn more about them, they train their employees and pull their finger out, leaving that fear behind.”

And that, in her opinion, is one of the essential things:

“Training employees is vital. If an employee knows she mustn't click on certain links received in an email, nine times out of ten, it will be enough to stop a cyberattack from happening, or to make sure that its consequences aren't too serious”.

In the workplace, we can reduce this level of employee insecurity by using tools that allow us to halt an attack even before it happens. Advanced cybersecurity solutions monitor the organization's systems in real time, detecting and stopping any suspicious behavior that could be harmful. Preventing attacks before they happen will help to reduce the stress that being the victim of a cyberattack can cause in an employee. ■

**“ADVANCED
CYBERSECURITY
SOLUTIONS
MONITOR THE
ORGANIZATION'S
SYSTEMS IN
REAL TIME”**



Xavier Mertens

CRYPTOJACKING IS ONE OF THE MOST BRILLIANT ATTACKS I'VE SEEN

The aim of a hacker used to be to steal or destroy information, yet today what they try to do above all is profit financially in exchange for information.

We can see how attacks are becoming more professional and businesses are being built around them. Some years ago, it wasn't so easy to buy ransomware or rent a bot to launch attacks. Xavier Mertens,

an independent cybersecurity consultant and renowned IT security blogger, insists on the importance of traditional security to combat these highly effective new threats. Mertens' voluntary participation in the SANS Internet Storm Center, the global cooperative system for warning against cyberthreats, gives him a great insight into the very latest attacks.

[Discover More](#)

PS: How can IT security professionals adapt to these new needs?

The usual protection measures are still important. If employees can stick to following typical security measures: implementing appropriate network segmentation, using secure passwords, configuring devices correctly and not exposing sensitive information or tools on the Web, I believe they could be protected against any modern threat.

Most security problems occur because people need to carry out everyday tasks, and are unaware of the basic measures required to protect them. Recently I tried to scan a document and, after checking the login credentials and firewall and ensuring that the printer worked correctly, I realized that it wouldn't work because the Server Message Block version 1 (SMBv1) protocol was configured, something that has already been widely disapproved of. As such, it is something you need to decide whether or not to enable. Users normally enable

the default settings as they don't know how to change them or they simply don't have time to do so and just want to get on with their day-to-day routine. But it is not so complicated, as industry experts, to resolve these basic problems and protect the security of tools that are as common in companies as printers.

PS: What is the Internet Storm Center? What is your role as an ISC Handler?

The Internet Storm Center is an organization whose aim is to monitor the Internet and ensure it operates properly. Using automated tools, we collect information for professionals in the sector, generate useful content in the form of a cybersecurity journal and try to increase awareness of the problem. For example, with the 'dshield' project, people can send their firewall records to build up our database and create a detection system based on repetition. We were able to detect the Mirai botnet because we have tools that showed activity peaks on specific ports. We are the 'Internet's firemen'.

PS: How can we avoid recent attacks such as those that are aimed at mining cryptocurrencies?

The protection remains the same as for other types of malware, because cryptocurrency mining is carried out with malicious code that runs on your computer. The standard advice still stands: have a cybersecurity solution that protects you completely and don't click or download unknown files. Nevertheless, I think that crypto-jacking is one of the most brilliant attacks I've seen. Criminals are moving from ransomware to mining because it is much less intrusive and you don't need so many resources to evade detection. With ransomware, you don't know if victims will pay the ransom because they may have backed up their files. With crypto-currency mining however, you are sure to recover your investment, and it is much less invasive. You can run mining on any type of device, unlike ransomware which is restricted to Windows, Mac or Linux, and the victim's system will still operate despite the attack.

**“THE INTERNET
STORM
CENTER IS AN
ORGANIZATION
WHOSE AIM IS
TO MONITOR
THE INTERNET
AND ENSURE
IT OPERATES
PROPERLY”**

A colleague at the ISC analyzed the power of his computer while mining cryptocurrencies. The fans and the CPU of the computer were always busy and running at full strength. So imagine the consequences that mining could have in a company with numerous computers: energy consumption increases, it has a significant impact on data center traffic and can even increase the office temperature.

PS: You have GIAC certification in reverse engineering malware. Should companies be investing in this type of analysis?

I don't think you should invest in reverse engineering unless

you have a big budget and a lot of time. The aim of companies is not to understand the behavior of malware, but to resume normal activity as soon as possible. When analyzing malicious files, we want to know why they behave as they do in order to generate a list of 'Indicators of Compromise' to share with other researchers in the sector and provide this intelligence to customers.

PS: How do you draw up an effective incident response plan?

Incident response plans are not easy to address, particularly if they are for companies that don't have the resources

or the right personnel. In my opinion, you can always start with the small things. The first step is to be prepared, increase awareness and involve all employees, and this is something that can be done by any company.

PS: As the deadline draws closer, how can companies prepare themselves for GDPR compliance?

The GDPR is designed to protect the privacy of users. So bearing this in mind, if you have implemented a comprehensive security strategy, if you know where the data is and how it is protected, and if you only have collected the information that

is strictly necessary for your business, the GDPR should not represent a problem for you. This regulation takes us back to basics, to some simple guidelines: encrypt your information, don't store passwords in public files, make sure databases are not exposed on the Internet, etc. Possibly the biggest challenge will be for small companies that don't have an inventory of all the information they possess, not just internal data, but also what they share with suppliers and users. Companies are now in the process of reviewing all the information they possess and we hope that they are taking the necessary measures to adapt to the GDPR. ■





Enrique Ávila

CYBERSECURITY ISN'T NEGOTIABLE: THE LOSS OF RESOURCES CAN MEAN THE END OF YOUR COMPANY

Enrique Ávila has a privileged point of view from his position: he is the director of the Spanish National Center for Excellence in Cybersecurity (CNEC), a key organization when it comes to the subject of cybersecurity. It integrates three core capacities: the university as a center for generating knowledge, companies for providing economic support and innovation, and the national law

enforcement agencies as the main users of technologies and knowledge in the fight against cybercrime.

Our subject, then, knows the evolution of cybercriminality in Spain like the back of his hand, as well as the efforts of this country to fight it, and the struggle to make companies and citizens aware of this subject.

[Discover More](#)

When we asked him whether there is an upwards trend, or to put it another way, whether cyberattacks are going to keep growing in 2018 and 2019, he didn't have to think twice: "In 2019, in 2020... Unless there's some kind of technological catastrophe, cybercrime will become more and more profitable, at least as long as the current circumstances don't change: the lack of territoriality in cyberspace, the use of pseudonyms by the actors, and the asymmetry of the resources used to cause harm or to illegally make money are all behind the exponential growth in these kinds of activities".

Ávila is no stranger to one of the most important Trojan horses for this kind of crime: carelessness and lack of awareness. And the fact is that "the perception of the risk is both low and poorly understood, both by citizens and companies". In fact, in his opinion, "companies must work on resilience and risk mitigation".

How can an SME protect its cybersecurity?

In any case, it is clear that many small companies may have trouble investing in their own cybersecurity, so "protecting SMEs, which generate the majority of jobs in our country, needs to be a State policy", although it is true that "both the Government and the INCIBE (Spanish National Cybersecurity Institute) are making an enormous effort to create an ecosystem of services, contact networks, awareness campaigns and training courses aimed at SMEs. It is also their responsibility to know about and make use of these resources".

But, moving beyond the abstract, how can a small company with very limited resources protect its corporate cybersecurity? For the director of CNEC, "the best thing would be to have an expert acting as an interface between the SME and the cybersecurity service providers.

But if the cost of this kind of service means that it isn't viable for you, it will always be more economical – and generally speaking more secure – to get these services from unmanned centralized infrastructures. However, with these shared infrastructures, there's a risk that, if they are the target of a cyberattack, you could become a collateral victim, even if you're not the main target".

In any case, the context has also changed. Until recently, protecting corporate cybersecurity depended (for the most part) on each company's wishes, and however they defined their own needs. Nevertheless, the definitive implementation of the GDPR, which imposes hefty fines on companies that aren't diligent with their cybersecurity, has forced a change in attitude for companies.

**“CYBERCRIME
WILL BECOME
MORE AND MORE
PROFITABLE, AT
LEAST AS LONG
AS THE CURRENT
CIRCUMSTANCES
DON'T CHANGE”**

Enrique Ávila is in no two minds: “Cybersecurity is not negotiable. Regulatory compliance when it comes to cybersecurity and the protection of personal data also affects companies. And, whether they like it or not, in our current society, the loss of IT resources is highly likely to mean the end of the company – whether it’s because the business can no

longer operate, because of the loss of reputation, or because of administrative or even penal sanctions, with the economic and social cost that this represents for our country”.

Thus, in this respect, the director of the Spanish National Center for Excellence in Cybersecurity points in two directions: making things compulsory and

raising awareness among the public, as well as among employees, because every company “has the obligation to invest in protecting their IT infrastructure, as well as training their employees in the subject, since a great deal of the company’s profits are derived from the use of this same IT infrastructure”. ■

“THE LOSS OF IT RESOURCES IS HIGHLY LIKELY TO MEAN THE END OF THE COMPANY”





Pablo González

THERE'S NO SUCH THING AS 100% SECURITY

Technology has evolved at a dizzying pace, and with it, the opportunities both for companies and for society. Pablo González Pérez, Technical Manager and Security Researcher at Telefónica, observes that these advances have also brought with them new risks and threats in the cybersecurity sector.

Pablo, with a broad experience in the industry, is the director of the Master's Degree in Information and Communication Technologies Security at the European University of Madrid, Microsoft MVP in 2017-2018 and 2018-2019, and author of such books as Ethical Hacking: Theory and Practice for Pen Testing.

[Discover More](#)

PS: What trends do you think have been important over the last few years in the cybersecurity landscape?

In my opinion, these are the most relevant trends:

- Criminals are taking advantage of cryptocurrencies to make a profit from malicious activities. Just a few years ago they were going completely unnoticed.
- The appearance of ransomware and the business model behind it has marked a before and after. Society has also begun to understand this kind of threat, since people are starting to notice the kinds of risks that are found on the Internet.
- The cases of data theft in companies. This is something that has grown and that, unfortunately, we will continue to see in the future.
- The appearance of the new data regulations designed to protect citizens.
- Attacks on critical infrastructures.

- The application of artificial intelligence in the field of cybersecurity. Without a doubt, within the next few years, cybersecurity and AI will go hand in hand.

- The increase in knowledge and awareness. This is something that is already happening gradually, and is starting to be noticeable, especially in younger generations.

PS: What differences have you seen in the types of attacks and threats?

The main difference is the use of the different technologies that have become available. A simple example is the case of phishing. It's something that's always been around, but these days we see how, thanks to QRLJacking or the use of OAuth apps, there's a different focus to the scam, and it's gaining access to accounts, in these cases, without even needing a password. With each new technology that comes along, new risks, or an evolution of the existing risks, come with it.

PS: Is it possible to prevent security breaches like the recent case at Facebook, where the personal information of 50 million users was exposed?

There's a saying that many professionals in the industry like to repeat, which is "everything is hackable". In other words, every company can fall victim to some kind of security incident. It's important that society and companies bear this in mind, and that they understand it. Establishing prevention measures in order to reduce the risk as much as possible is vital these days, but not everything can be preventive: there must be an alignment of risks between preventive and reactive measures. There's no such thing as 100% security, and so we must keep working iteratively on the ways that companies protect themselves. We must also add preventive measures, align reactive measures, and create a base in which people that belong to the organization are involved in the organization's security.

“EVERY COMPANY CAN FALL VICTIM TO SOME KIND OF SECURITY INCIDENT”

PS: The IoT will increase the attack vectors. How can we protect a world in which everything is connected?

Protection must be shared between the provider and the consumer. In my opinion, security mustn't be tackled by just one role, since in the equation there are at least two roles. If both parts take on their responsibility in terms of protecting information, we'd be much more robust when it came to risks.

On one hand, including security from capturing requirements, from the design of the systems, is something that would provide a major level of maturity to the process. This is something that has a direct effect on the manufacturing costs, but that in the long run benefits everyone, and provides a quantifiable return. A secure development life-cycle brings maturity to the process, which is the minimum we should aim for. At each stage of the process, elements such as the following can be added:

- The gathering of security requirements.
- Threat modelling.
- Analysis of the attack surface.
- Static and dynamic analysis.
- Code revisions.
- Pen testing.
- Testing.
- Strengthening secure settings.

Logically, the elements discussed pop up in the different phases of this kind of methodology, and bring an extremely interesting value to the creation of software and systems. The idea is simple: think of security from the very beginning. On the other hand, when the consumer makes use of the system, they must understand the risks and threats to which they are exposed simply by using this technology. This is something that society is learning, though not at the speed with which new threats and risks are appearing in our lives.

**“THE CONSUMER
MAKES USE OF
THE SYSTEM,
THEY MUST
UNDERSTAND
THE RISKS AND
THREATS TO
WHICH THEY ARE
EXPOSED SIMPLY
BY USING THIS
TECHNOLOGY”**

PS: Do you think attacks are getting more complex or that the cyberattackers are becoming professionalized?

In some cases the attacks are more complex; they exploit vulnerabilities or take advantage of more complex bugs, although in other cases this isn't so. At times it's tempting to think that a security incident is the result of very complex tactics, whereas in actual fact, it turns out the attackers managed to get in using basic phishing tactics on an employee, or because someone within the organization extracted the data, without an appropriate traceability control. On the other hand, attackers are becoming more specialized, and know how to use the latest trends in order to turn a profit. This is quite normal, since there is an increasing amount of research, more and more information that is accessible, and the volume of data in the security sector grows every day.

PS: Do you think advanced cybersecurity solutions are a priority when it comes to protecting endpoints, now that the number of endpoints is always growing? What role do you think predictive intelligence will play in cybersecurity solutions in the coming months or years?

If we understand cybersecurity as a model in which every layer and every area must be protected – similar to an in-depth defense model in a military environment – any correctly configured solution that helps to improve security, and to reduce the threats and their impact, is a priority. Without a shadow of a doubt, predictive intelligence will help improve cybersecurity solutions. It will become one of the cornerstones for tools within the industry. The importance of getting ahead of situations and risks will be fundamental to the continual improvement of cybersecurity.

PS: Your specialty is pen testing: What tools do you use to carry out these analyses?

You need to have a set of environments and tools that you feel comfortable with. The specific names aren't important. What matters is exploring the needs that must be fulfilled and what a specific tool can bring at each moment. Of course, in many environments you end up using the same tools and your own manual dexterity. You need to keep an eye on the new tools that appear and that can make your job easier.

“ATTACKERS ARE BECOMING MORE SPECIALIZED, AND KNOW HOW TO USE THE LATEST TRENDS IN ORDER TO TURN A PROFIT”

PS: How important are ethical hackers in the current business world?

Ethical hacking is a fundamental part of the current business world. The fact that companies need to feel safe in a digital environment in order to go about their business means that ethical hacking is vital to improving security, both of this digital environment and of the companies' activities.

PS: You're also a lecturer in the cybersecurity sector. How important is teaching in this industry?

Awareness, knowledge, training... they're all the base of security culture for any company – or at least they should be. Security is fundamental for organizations and Internet users to be able to carry out their activities naturally and safely. Teaching

has an important role in the industry, and can come in many forms: universities, private companies, books, blogs, articles, magazines. It can even be self-taught. What's more, a lot of the time you need to be self-taught in order to assimilate different knowledge,

“THE IMPORTANCE OF GETTING AHEAD OF SITUATIONS AND RISKS WILL BE FUNDAMENTAL TO THE CONTINUAL IMPROVEMENT OF CYBERSECURITY”



to put it into practice in controlled environments and to be able to better understand the possible situations, risks, and threats.

Employee training is also one of the bases for creating a security culture within an organization. It is vital for the organization and, undoubtedly, the most complex thing to achieve. Initiatives such as gamification, innovation, and challenges can help turn employees into driving forces for security in companies.

PS: How can a company increase its cyber-resilience? What security measures are indispensable?

There are different ways, but the most important is to really want to be resilient. In my opinion, there are a few things to bear in mind:

- Having a team that responds effectively and efficiently to any incident. One that is trained and that can analyze possible situations and make decisions.

- The use of prediction and intelligence techniques is vital for companies these days.

- Correlating events and cases will give a global vision of the situation.

- Having recovery measures that allow an organization to return to a previous state in case of a serious incident.

What's more, we mustn't forget that having knowledge within the organization is also vital. ■



**“EMPLOYEE
TRAINING IS ALSO
ONE OF THE BASES
FOR CREATING
A SECURITY
CULTURE WITHIN AN
ORGANIZATION”**

We live in a digitalized society. We're experiencing a transformation of social relationships, of the business world, and of how governments are run.

In order to protect our digital lives, and those of our businesses, cybersecurity has become a requirement of our daily activity. And likewise, its management needs an in-depth review, with new security models.

With the aim of discovering needs, revealing trends, getting to know the points of view of the different structures that make up our society, at Panda Security, we held our first advanced cybersecurity summit back in May. The Panda Security Summit 2018 had cyber-resilience as its

focalpoint. Among the audience of over 400 attendees were CISOs and CIOs of large Spanish and European companies.

Silva Barrera hosted the event, which served as a framework to look at the latest cybersecurity trends – attacks, and how to protect against them all along the security chain, as well as the overall state of the sector – from the point of view of analysts, public institutions, and private companies.

Throughout the lectures and workshops, the participants were able to get an idea of the cornerstones needed to reach the highest levels of security in organizations. The importance of being resilient when it comes to security was widely recognized as a

fundamental characteristic, as well as being the leitmotif of the latest report published by Panda Security, presented at #PASS2018.

All of the speakers also shared their ideas and experiences of how to prevent attacks, how to get back to the original state after an attack, and how to mitigate the effects of an attack using a good response strategy. The common thread running through all the strategies analyzed was prevention, detection, containment, and response.

In this Ebook, you've been able to read a few of these reflections, taken first hand from the participants in the Summit, such as Javier Candau, head of the Centro Criptológico Nacional (CCN-

CERT, the Spanish National Cryptologic Centre) who focused on the challenge that cybersecurity represents in Spain.

Ian McShane, Research Director at Gartner explained in his lecture that the challenge for 2019 is to reinforce prevention, especially in the endpoint protection strategy. “The endpoint needs something more than an antivirus; endpoint detection and response (EDR) technologies are the key, as they offer a traceability which is indispensable for analysis

and prevention. But these technologies aren’t going to replace humans; we still need analysts,” he explained. Nikolaos Tsouroulas, Head of Cybersecurity Product Management at ElevenPaths in Telefónica explained that “technology is necessary, but people are even more important. Security professionals are the most valuable investment in this area.”

Nicola Esposito, Director of Deloitte’s CyberSOC EMEA Center also participated in the event. He highlighted factors

such as the application of threat intelligence platforms, the creation of threat detection controls, and perimeter monitoring with automated alerts, but always with a fundamental role played by humans.

Finally, the director of the laboratory PandaLabs, Pedro Uría, put forth the keys for business security, protection and resilience, now that malware is no longer the problem. Instead, hackers are the future challenge of cybersecurity, as they use more complex methods.

After operating for 28 years, Panda Security held its first cybersecurity summit. A must-attend event for all cybersecurity professionals. Don’t miss out on the next edition: Panda Security Summit 2019. The European Cybersecurity Hub!

[Discover More](#)

[Play Video](#)



More Information:

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

By email:

communication@pandasecurity.com