Executive and Information Security

Sophistication of attacks and complexity of IT environments have risen rapidly, addressing this challenge, requires solutions that cut across strategy, operations, risk management, legal and technology functions.

Today in the organizations, at any levels, we are agree on the fact that information is the business, access to reliable information is an indispensable component for driving a successful business.

The business thinker Peter Drucker in his book "Management Challenges for the 21st Century", published in 1993 wrote "The diffusion of technology and the commodification of information transforms the role of information into a resource equal in importance to the traditionally important resources of land, labor and capital". Even in the fiction, film The Sneaker 1992, the hacker Cosmo shout, against the security team lead Martin Bishop, a prophetic sentence "There's a war out there, old friend. A world war. And it's not about who's got the most bullets. It's about who controls the information". During these years, value and dependence on information have increased exponentially and this trend will continue into the foreseeable future. In this scenario organizations need to reverse the approach used for cyber risks; instead of starting from technological vulnerabilities they should first protect the critical assets with a business approach.

This means implement a corporate data classification program, in this way organizations may focus cyber security efforts and policies on their most critical information assets. Even in this line, organizations need to evaluate their cyber risk profile across the full value chain, clarifying expectations with vendors and strategic business partners.

Business approach means also that cyber security represents a business opportunity, so said, it is very important that marketing is involved in order to create end-to-end customer experiences that are both convenient and secure.

Till today organizations approached cyber security increasing defense around their perimeter with sophisticated technology when they have to reorienting security architectures from devices and locations to roles and data. We need to move from the perimeter defense approach to protect the data.

To be effective organizations must make cyber security a key part of the business case for major initiatives or new-product introductions and also strategies that may address not only new threats but also evolving business.

In order to address in a proper way these issues, cyber security must be a constant subject on the agendas of boards and executives. To win this challenge, executives must engage in an ongoing dialogue to ensure their strategy continually evolves and realizes the appropriate trade-offs between business opportunity and risks.

All the organizations need to make all these issue a broad management initiative with a mandate from executives and operational levels in order to protect critical information assets without placing constraints or blocking business innovation and growth.

in online shopping and entertainment.

Nicola Sotira
General Manager GCSEC
The new European General Data Protection Regulation (GDPR) entered into force on 24 May 2016 is posing a number of questions to the European organizations are called upon to comply by 25 may 2018. GDPR is directly applicable and binding to all European member States, without a national law review, and is applicable also to foreign companies that provide services or products inside the European Union.

The GDPR presents many challenges. It introduces new obligations like the communication of personal data breaches, adoption of a risk-based approach, “right to be forgotten” and right to data portability, “privacy by design” principle. The GDPR identifies also a new figure, the Data Protection Officer (DPO) that has to ensure a correct privacy management inside the organization.

The adoption of a DPO is not a mandatory requirement for all organizations. In particular, the GDPR requires a DPO only for public authority or body and private organizations in which “the core activities of the controller or the processor consist of processing on a large scale of special categories of data” (i.e. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs).

The role of DPO, with specific tasks like to inform and advise the controller, monitor compliance, to be point of contact with Supervisory Authority and data subjects, will play a strategic role. Which is the perception of European organizations? Will the DPO be design also by the organization for which it is not mandatory? In accordance to the 37 articles, the DPO shall be designated on the basis of “professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks”. Which are the professional qualities, capacities and characteristics by which the organization will identify the DPO? Does a similar role already exist inside the organizations?

What they are learning. Maker Faire celebrated 150 Faires in 2015 alone and has reached over 1.5 million attendees globally since it launched in San Mateo, California in 2006, less than a year after the publication of the first Make: Magazine. The tenth annual Maker Faire Bay Area welcomed some 1200 maker entries and 145,000 attendees. In this event GCSEC and Poste Italiane will launch an awareness campaign on the proper use of Internet and digital services.

**ATM: A look at the future and emerging security threats landscape**

Global Cyber Security Center organized a workshop on ATM security on 22nd of September 2016 in Rome, in collaboration with Auriga, Braintech, Consorzio Bancomat, Diebold Nixdorf, Kaspersky Lab, NCR, Security Brokers. At the workshop, the cyber security experts discussed on safety of ATMs. In the last few years the typology and numbers of attacks against Automated Teller Machine (ATM) systems have increased. The workshop was a moment for exchange experiences of national and international experts. During the workshop, were discussed actual and future attack scenarios, techniques and tactics adopted, actions to put in place to enhance ATM security level and compliance challenges that we should face. The workshop was the occasion to present the study “ATM: A look at the future and emerging security threats landscape” coordinated by GCSEC.

**Five Tips to reduce dwell time**

by Scott Penney, Director Cyber Security Solutions, BLUECAT

**201601 Threats Report - Summary**

by ADS Group

**A Global Vulnerability In A Digital World**

by published on Forbes.com (12 September 2016)

**Globalization of networks towards the empire of knowledge**

An interview with Roberto Panzarani Professor of Innovation Management by Massimiliano Cannata - Technology Innovation, Training and Security Culture Reporter

**A SURVEY TO EVALUATE THE IMPACT OF THE EU GENERAL DATA PROTECTION REGULATION ON ORGANIZATIONS**

by Elena Mena Agresti, GCSEC

**Global Cyber Security Summit**

Date: 31 October - 1 November, 2016

Location: Rome, Italy

http://goo.gl/lg7qjW

Global Cyber Security Center is proud to be partnering with Skytop Strategies on their upcoming Global Cyber Security Summit taking place at The Cavalieri in Rome Italy October 31-November 1st. Engage with heads of technology, security, law, risk, governance, and audit & compliance experts on reframing cyber security through strategic innovation. Discover how integrative practices build resilience capacity and empower companies to proactively stave off attackers while applying innovations in resilience planning designed to get ahead of rapidly emerging global threats.
In addition to organizational changes, such as the role of the DPO, the GDPR requires substantial changes to processes and activities of companies to respect, for example, the right of data portability that allows users to automatically transfer their personal data from one provider to another.

In accordance to the 20 article, the data subject has the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided”. Have the organizations already identified all data subjected to portability? The organizations have to align their processes and their systems to the new privacy system. How and in which way will this changes impact the organizations?

With the implementation of GDPR, the organizations have to implement an “impact assessment”, an evaluation of privacy impact, before to process personal data to mitigate risks and ensure a correct personal data protection. What is the perception of European companies? This change will impact significantly on business processes?

In case of a personal data breach, the organization have to notify the personal data breach to the supervisory authority, not later than 72 hours after having become aware of it. Any violations make the organization subject to administrative fines much higher than those defined by the actual privacy regulation in Italy. The administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year. This change will have produced an increase in awareness about the security issues of personal data?

To try to answer to these and more other questions, the foundation GCSEC of Poste Italiane and Europrivacy, an European observatory on the new EU regulation on Personal Data Protection, will publish a survey aimed to measure and evaluate the impact that the adoption of the new European Regulation Policy will determine for the public sector, the big companies and SMEs. In fact, the survey aims to evaluate the level of knowledge of the new GDPR and perceived the implantation impact of GDPR in Italian and European organizations.

The survey will focus on the processes to be put in place to respond to the new regulation, the organizational and training aspects, the resources and skills required. Will be also analysed the new figure of DPO that will play a crucial role within organizations. You will be able to answer survey on our GCSEC or Europrivacy website (“http://www.gcssec.org" "http://www.europriacy.info”) by the middle of October.

---

**FIVE TIPS TO REDUCE DWELL TIME**

*by Scott Penney, Director Cyber Security Solutions BLUECAT*

Dwell time is arguably the most accurate indicator of an enterprise's security. It can determine how good you are in finding and eliminating actual breaches. Some indicators are less reliable. For example, the number of breached systems might either indicate your systems are well protected or, it might mean there are gaps in your ability to identify intrusions. On the other hand, dwell time is critical for an attacker to reach its goal, because an attack must go through all the steps of a "Kill Chain", which requires time.

Stealth is the number one tool in an attacker's arsenal – a breached system should look and behave as normal as possible to avoid detection. To keep their activities under the radar, cyber attackers use common protocols and services to communicate with Command and Control centers, to avoid attracting attention of common detection methods. Using covert channels such as DNS exfiltration and posting innocuous looking messages or images to social media to be picked up by the attacker later are becoming increasingly common for avoiding detection.

Attackers have done a great job authoring malware that is very “low signal” in an effort to stay hidden. Enterprises on the other hand end up sorting through all the noise of the various security technologies they have in place to find that signal. This is basic physics - if you design your detection scheme to be (2013-2015) also im working on OPAnonHQ, which is against the huge amount of profit they make with the anonymous idea, since they need about 200-000 dollars a year to run the servers (confirmed stats below)

Purchase/Sale Value: $452,520 USD
Daily Revenue: $1,240 USD
Monthly Revenue: $37,734 USD
Yearly Revenue: $452,510 USD
Daily Unique Visitors: 261,001
Monthly Unique Visitors: 7,944,048
Yearly Unique Visitors: 95,265,365
OpWhales, OpKillingBay-EU, OpSeaWorld – For this operations, we provide network support via creating media and assisting and bringing sites offline.
Op Gabon – To support Gabon population, by bringing websites offline and spreading awareness through the social media.
Op NoDap – As AnonRising/Risingsquad we provided media mirrors and IRC support for this operation and shared awareness via other social media platforms. And many more OPS which are still going on.

Vulnerability patched in wordpress theme that allows unrestricted uploads
http://goo.gl/f1JuwmQ

WordPress theme publisher DynamicPress fixed a flaw Monday that let anyone upload malicious files to sites running its business-themed Neosense WordPress templates, compromise the site and possibly the server hosting it. Walter Hop, security researcher with Netherlands-based company, Slik, made the discovery last week. The flaw impacts version 1.7 of the Neosense theme. On Monday, DynamicPress released a 1.8 version update that patches the vulnerability. Hop publicly disclosed the vulnerability Monday. See more at: Vulnerability Patched in WordPress Theme That Allows Unrestricted Uploads https://wp.me/p3AjUX-voK

Yahoo Confirms the Breach of 500Mn Online Credentials
http://goo.gl/p7IoTw

Back in August, the hacker responsible for dumping hundreds of millions of MySpace, LinkedIn and other credentials online in recent months claimed to have put up for sale 200 million Yahoo log-ins. Yahoo said at the time that it was “aware” of the incident, although it didn’t initiate a user-wide password reset.

Now, the online giant—which is in the process of being acquired by US telecoms behemoth Verizon, has confirmed the situation, but the breach is larger than expected, and Yahoo said that the heist was carried out by a state-sponsored attacker..

A Brazilian Infosec research group, Morpheus Labs, just discovered a new Full Disk Encryption (FDE) Ransomware this week, dubbed Mamba. http://goo.gl/olK6gS
too sensitive to the signal it will get overwhelmed by the noise, giving nothing but endless false-positives that erode the confidence in the scheme itself. On the flip side if you design your detection scheme to be too insensitive, you will never find the signal that indicates the compromise.

With that being said, we have put together five basic tips to reduce the Dwell Time that typically ranges between 200-250 days as cited by a number of surveys done recently.

1. Enterprises should co-evolve with the attackers and understand that traditional firewalls or signature-based detection methods will do little to protect against the new generation of threats.
2. As attackers are opting for indirect methods of communication through legitimate services, enterprises should focus their efforts to understand their "normal" by closely monitoring internal and external traffic on their network. Most enterprises just capture external traffic through web proxies but have no visibility into the internal network.
3. Once the baseline is established, any deviation from expected behavior should be scrutinized further to look for signs of suspicious activity.
4. Enterprises should assume that they will be breached and prepare for it, which means that sufficient resources should be allocated into detection and mitigation as opposed to just focusing on prevention. A recent survey of over 300 large enterprises conducted by UBM and commissioned by BlueCat revealed through a joint webinar that:
   - 93% of organizations use anti-virus and anti-malware tools
   - 82% use perimeter firewalls
   - 65% use intrusion preventions systems
   - 52% use unified threat management systems
5. Traditional security best practices such as hardening all systems, performing risk management analysis and prioritizing the patching of critical and vulnerable systems consistently still goes a long way in shortening dwell time.

About BlueCat
BlueCat delivers software-based DNS solutions to enable enterprises to automate, manage and secure their networks. Leveraging DNS, BlueCat provides the foundation for enterprises to build scalable and secure networks that can pivot and flex to efficiently respond to complex business demands. We improve efficiency by enabling compliance, data management, and automation at scale. We deliver value by enabling our customers to build once, then evolve and change without having to re-architect or re-buy.

Mamba, as they named it, uses a disk-level encryption strategy instead of the conventional file-based one. This may be just the beginning of a new era for the Ransomware.

In this article, Renato Marinho (@renato_marinho), the researcher responsible for the finding, explains more about this new threat [1]

About Mamba
"You are Hacked". This message is all that remains of the victims of this new Ransomware. To get the decryption key, it’s necessary to contact somebody through the informed e-mail address, give the ID and pay 1 BTC per infected host. Without that, the system even starts. For the matter of this article, we will call this Ransomware “Mamba”, a snake with a paralyzing poison.

It seems that the disk level Ransomware family is growing. A similar Ransomware, called Petya, got famous march this year because of the disk encryption strategy, although some analysis [2] says that the malware encrypts the master file table (MFT) and not the data itself. But Mamba Ransomware differs from Petya exactly at this point. It uses a full disk encryption open source tool called DiskCryptor [3] to strongly encrypt the data.

Chinese Hackers Remotely Control Tesla Cars
http://goo.gl/7aY6Gw

Chinese researchers have discovered major security vulnerabilities in several Tesla car models, allowing them to remotely apply the brakes, open the boot and perform other actions which could put drivers in danger.

A team at Shanghai-based Keen Security Lab – part of Chinese web behemoth Tencent – demonstrated the remote hacks in a video on their site. In it, they open the car door, pop the sunroof, adjust the driver’s seat and turn the indicators on – all while in park mode.

However, more dangerous is the cyber-attack that allows them to fold the car’s wing mirrors when it changes lanes whilst driving, and another which brakes the car when in motion.

The team was tight-lipped on how they carried out the proof-of-concept attacks, although it worked on “multiple varieties of Tesla Model S” running the latest firmware at the time and they said it “is reasonable to assume that other Tesla models are affected.”

“As far as we know, this is the first case of remote attack which compromises CAN Bus to achieve remote controls on Tesla cars,” Keen Security Lab claimed.
Cryptography is not enough. Who decided to protect his data only by Android file system encryption, was wrong. It has been discovered a leak in the most commonly installed CPU on Android devices, that can be combined with some application vulnerability to obtain the encryption key which has been used to decrypt the protected content.

The credits goes to security researcher Gal Beniamini, who has worked in IDF (Israel Defense Force). He estimates that 57% of the Android systems is being impacted. This value has been disputed by the operating system developer (Google) who said it is 45% (only Android 5.0+ devices). Indeed, the main issue is that more than 1/4 of the impacted devices will likely stay vulnerable 1 60% of attacks to mobile devices targets Android operating systems, which is installed on about 1/3 of company mobile devices2. Let’s try to figure out what would happen if data stored on a medium size company’s mobile device, protected with a vulnerable encryption system, are accessible by an attacker or, in the worst case, by a competitor: interruption of activities, data theft, profit loss and generally business damages. A huge amount of potentially critical information of different kind (industrial secret, company projects, applications and strategic documents) might be used for malicious purposes which would affect both the Company operations and reputation.

A worry might become an issue, and an issue might become a cost (7.880$/device3). The step toward the catastrophe is short and goes through a recently discovered bug in the Qualcomm Snapdragon processor which – if combined with another application vulnerability – can lead to unauthorized access to the storage encryption key and thus to the data

---
stored in the device.
To figure out how this can happen, it's crucial to understand how file system cryptography works on Android devices.
In order to create the encryption key, Android uses two elements:
- the PIN code (or password or swipe pattern) chosen by the user;
- a key generated by the KeyMaster, which is a trustlet, i.e. an application located in the TrustZone, a kernel restricted access area.

The key generated by the KeyMaster is stored in the TrustZone as well.

So, to obtain the encryption key it is "enough":
- to discover the PIN/Password/swipe to unlock the device;
- to gain access to the KeyMaster.

About the first point, it's been demonstrated that PIN codes and swipe patterns do not properly protect devices and passwords are often easy to deduce/discover.
About the second point, it must be considered that the KeyMaster is located in the TrustZone, which is accessible only by an Android user-space kernel module. In the Qualcomm CPUs, this module is called QSEECOM (Qualcomm Secure Execution Environment COMmunicator).

The combined exploitation of CVE-2015-6639 and CVE-2016-2431 vulnerabilities allows to break in the safe area.
The first vulnerability concerns the trustlet Widevine, a software to play encrypted and copyrighted-protected media. As a trustlet, located in the TrustZone, the app can be managed only by the means of the QSEECOM. Exploiting the bug allows to directly use the QSEECOM, but does not give access to the other apps in the TrustZone.
The second vulnerability concerns the QSEECOM: by exploiting it, a Privilege Escalation is fired to gain access to the TrustZone, to its contents and to all the trustlets, KeyMaster included.
Facing this scenario just by hoping to not become a target, it's definitely not an option.
Within the company context, there are some best practices which allows to lower the risk of losing data stored on mobile devices.

Prevention can be a pain, in some cases. For this reason, a business priority assessment should be considered. That’s what Risk Analysis is for.

For the purpose of this work, it has been considered the threat “Theft of Devices, Storage Media and Documents” in a Company counting about 250 employees. The analysis has been performed by using a propriety risk analysis framework, whose result has been to estimate the risk as CRITIC, due to a not-so-high likelihood of occurrence (threat agent should have fairly good skills) but a catastrophic reputational and economic impact.
This data allows you to process a corporate strategy that should include at least:
- to schedule emergency interventions, in spite of patch management and corporate change management plans;
- the immediate application of containment mitigations and the implementation of strategic Best Practices;
- the prompt activation of threats-focused monitoring channels.

The approach to choose is crucial: Security must not be considered as a “to-be condition”, but as an enabler and a process (or a control set) applicable to all the actions performed in the IT field, so to become an inner part of the whole range of business processes, and which can grow, change and improve itself over time, according to the threats landscape.

---

4 codice T0.16 nel BSI Threats Catalogue
Whether you’re a middle market or multinational corporation with an entirely automated infrastructure, cyber security breaches have become an inevitable threat to businesses and individuals worldwide. Cyber security measures have become not an option, but a requirement, in an increasingly digitized corporate environment. “Over the last two or three years, companies in every industry segment and tier have confirmed they have suffered cyber attacks,” Jennifer Archie, a litigation partner of Latham & Watkins specializing in large-scale data breach response, says. The risks vary from minor annoyance to sizable devastation. Cyber attacks may result in stolen information, loss of funds (the 2016 Verizon Data Breach Investigations Report (DBIR 2016) reported that 89% of 2015 data breaches had a financial or espionage motive), email compromisation, malware infection and even widespread power outages, as we observed in the December 2015 BlackEnergy attack against a number of Ukrainian energy companies.

In our continuing evolution in the Information Age, we may have simplified administrative functions, increased internal efficiency, and maximized accessibility on a global scale, however, we have inevitably opened the floodgates to a swarm of hackers, phishers, viruses and other mal-intended intruders. “It is ironic,” Robert Katz, Founder and Executive Director of the Innovation Intelligence Institute reflects. “If we look at all of the technology that creates freedom and independence, it actually creates technological dependence. We hyper-modernized and hyper-connected—we became all digital, all electric, all the time. While this hyper-convergence heightened convenience, it simultaneously heightened vulnerability.”

What happens when a corporation suffers a major breach? Well, that depends on the jurisdiction. “What is illegal in one country is not necessarily illegal in another,” Ira Winkler, President of Secure Mentem, explains. “Some of the data breach laws are requiring the reaction from the companies, mandating reaction by the companies, but they are not necessarily mandating security.” What does that mean for corporate stakeholders? In the U.S., companies are required to report cyber breaches to their board and corporate shareholders, so in this country, if a corporate database holding our personal information is compromised, we’ll typically hear about it.

The World Law Group published a comprehensive list of mandated corporate response by country in “The Global Guide to Data Breach Notifications.” As the report shows, if you’re invested in an Australian, Greek, or Colombian entity and they suffer a cyber attack, they aren’t legally obligated to notify you or regulators. In China, however, the Consumer Rights Protection Law states that if a disclosure or loss is even suspected, businesses are required to adopt remedial measures. The only formidable defense against these kind of attacks, whether direct or indirect, requires a holistic approach. Effective cyber security must balance risk management, technological innovation, human capital and tactical governance.

A Game Of Cat And Mouse
As the founder and executive director of the Innovation Intelligence Institute, Katz helps “infuse, both internally and externally, innovation into otherwise not innovative organizations.”

“Typically in organizations, they only collaborate internally or with pre-existing stakeholders,” he explains. “To be able to really solve any problems, we have to start looking at things differently and start to reach out to non-traditional stakeholders.” He often uses one key phrase when describing an effective cyber defense: hyper collaboration. “To solve the cyber problem, we tend to really look at it as a technology issue, but it is really much more than that,” he says. “It’s a complete societal issue.”

Increasingly, corporations are turning to third-party, off-site data centers to further encrypt sensitive information. (A persistent phrase in cyber conversation from elementary to federal levels, it's impossible to avoid mention of “the cloud.”)

The cloud can definitely be secure and in some cases, it can be more secure than some on-prime environments, but there are several factors that it can depend on,” David Cass, CISO of Cloud & SaaS Operational Services at IBM explains. “Hopefully you have good security practices already and you're mapping the security practices over. The key to cloud is the concept of shared responsibility between the Cloud Service Provider (CSP) and the customer.
Depending on whether you are doing IaaS, PaaS or SaaS, the delineation or who is responsible for what portions of security varies. This is an important conversation to have with your CSP."

The three most commonly used cloud services fall under three categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). An IaaS model, the most fundamental cloud service, houses basic computing infrastructure off-site; virtual machines allow users to access those off-site infrastructures as they would a physical machine. The PaaS model provides a computing platform for software developers with automatically adjusting capacity to accommodate their hardware/software needs virtually, eliminating the need to purchase and manage layers manually. SaaS cloud services allow users to house and operate software off-site, saving both space and time dedicated to maintenance.

Housing infrastructure, platforms and software off-site toes the line between privacy and security. While cloud-based services “make hardware and operational management of technology systems somebody else’s responsibility that specializes in them,” as Cass describes, without proper data encryption, any information or service stored on the cloud may still be at risk without proper security practices already in place.

On the same front, Katz believes artificial intelligence (AI) will provide more resilient protection from cyber threats. In the ongoing game of cat and mouse—while we rush to patch a broken window, hackers are already picking the next lock—we need to begin thinking like the enemy. “The adversaries have the advantage because they have massively parallel computing because they are massively collaborating. So must we,” Katz says. “So that is where AI comes in.”

AI may create a more reliable security system, but you can’t automate a human to set the alarm before leaving for work. In cyber terms, we can’t underestimate the importance of fostering preventive behaviors on an individual level. “We have to have users be more careful about how they use the technology,” Katz continues. “We have to have social scientists talk about how we are able to social engineer and trick people: behavioral scientists, human resource people and technologists as well. So it takes a village.”

Cass agrees: “At the end of the day, you can out-source anything really except for accountability.”

The Achilles Heel
An effective cyber security strategy is a “team effort,” says Guy Filipelli, founder and CEO of RedOwl, a cyber security/risk management company. “It is often a combination of information security, physical security, technology or IT, legal, and potentially risk or HR and then at one point, the leadership of the institution.”

Corporate leaders are responsible for strategizing a cyber security plan, from conceptualization to implementation. Yesteryear’s silos are busted open by the Information Age; because the modern corporation is entirely digitized, employees at every level need to collaborate to avoid becoming the weak link.

The list of human vulnerabilities is endless—insider sabotage, improper shutdown of company computers, common password choice (SplashData’s list of Top 25 Most Commonly Used Passwords for 2015 proves that we all learned nothing in 2014...123456,” “password,” and “12345678” continue to top the list). The DBIR 2016 found that 13% of people tested clicked on a phishing attachment.

Educating the workforce is a good first step, but a learning curve also needs to be considered, says Dan Swanson, President of Dan Swanson & Associates and a 26-year internal audit veteran. “I think there has to be a continual learning strategy for your organization to be truly successful over the long-term,” he says.

That being said, the ongoing war against internal human error is only half of the battle; technological vulnerabilities still account for a significant portion of cyber security risks. On a software level, the Common Vulnerabilities and Exposures (CVE) system compiled by the U.S. Department of Homeland Security, shows that the 10 products with the most vulnerabilities account for 85% of successfully exploited traffic. In order of most to least vulnerable, those products are Mac OS X, Linux Kernel, Firefox, Chrome, iPhone OS, Flash Player, Internet Explorer, Debian Linux, Windows XP and Windows Server 2008.

Manning The Barracks: Keeping Cyber Threats At Bay
The NSA hack earlier this year proved that even federal agencies are prone to cyber attacks; not even a government-level organization with security in the name has forged an impenetrable cyber defense.

To best protect a company’s digital infrastructure, an effective cyber management team requires a certain skill set. Barclay Blair, Founder & Executive Director of the Information Governance Initiative, compares the indispensable qualities of influential information leaders to those of emergency workers. “There is a dance of really understanding the long view while trying to fight the fires, which is obviously the same for people who work in traumatic and stressful situations. If they don’t, they don’t last,” he says, adding that they must distinguish between “the threats that are faced by the organization that must be triaged immediately, and separating those things from the things have to be, and should only be addressed, as part of the longer term plan.”

The National Institute of Standards and Technology (NIST) cyber security framework provides tentative guidelines to design effective cyber defenses and reactionary protocol. "Cyber Threat Intelligence also help to determine the effectiveness of an ongoing effort, requiring standards and assessments to be compared with configurations, best practices and most importantly, common sense," says Ariel Evans, an American-Israeli cyber security expert, formerly the CISO for a major telco company in the United States.

“I do believe that organizations have a right to defend,” Araceli Treu Gomes, a principal subject matter expert in cyber security and intelligence says, adding, “I’m not sure if taking an act of offense constitutes as defense. Furthermore, I don’t think the business side of the industry or the risk-management side of the industry are competent enough to understand the collateral damage that can and will be caused by hacking back.”
Guarding The Fortress: Reinforcing Cyber Defenses

Now imagine a situation in which the enemy resides within your borders. So is the case of Advanced Persistent Threats (APTs), in which a hacker embeds themselves within a digital infrastructure for extended periods of time to conduct long-term cyber espionage. Serrin Turner, partner of Latham & Watkins and a member of the firm’s Cybersecurity and Data Privacy practice group and formerly the lead cyber crime prosecutor from the U.S. Attorney’s Office in Manhattan, describes how APTs pose an evolving threat.

“Organized crime groups, which in the past have typically focused on theft of credit card data and personal identity information, are increasingly using APT tactics that are traditionally associated with nation-states—burrowing into corporate networks to steal trade secrets or other information that can be quietly monetized through insider trading or other means,” he explains.

Not all APTs are contained by a timeframe, however. “There have been cases where the people you would consider as APT get in and then get out really quickly,” Winkler says. He defines an APT as “a very motivated and skilled attacker who is willing to put relatively unlimited resources towards obtaining their goals. They are adaptive in that they see what protection mechanisms [their targets] have and then they try to avoid those protections and keep trying until they get around it.”

NGLF: initialized & active

Establishing a set of digital obstacles for potential APTs is hardly the first step in an effective cyber defense strategy, according to Swanson. “It starts with a team, with a set of policies and standards. Like any large corporate effort, regardless of the industry, you need a capital investment program, a large operating budget that is appropriate to the organization and the risks involved.”

Cyber insurance can potentially contribute to an effective cyber defense strategy. The Insurance Information Institute found that stand-alone cyber insurance policies typically feature crisis management; directors, officers and management liability; business interruption; cyber extortion; and loss/corruption of data. Statistics show that more and more often, corporations are turning to insurance brokers to fortify their defenses. Major insurance broker Marsh estimates that U.S. cyber insurance was worth over $2 billion in gross written premiums in 2014, with some estimates predicting that figure could potentially triple by 2020.

Still, not all experts believe that cyber insurance is a cost-effective risk reduction strategy. Gomes believes insurance brings up “the darker underbelly of risk management.” The question, she said, revolves around whether or not insurance companies should be in the business of mandating and dictating controls. “Are we going to start buying cyber insurance the way we do homeowners insurance or like rental car insurance? What is it going to look like?” she asks. “What is your risk management position as you go to acquire it?”

Placing The Defense On The Offense

As cyber criminals evolve to exploit in-place defensive measures, C-Suite executive and director response need to shift from “a reactive to proactive approach,” according to Evans. “It is no longer adequate to speak solely in terms of technological vulnerabilities such as insufficient patching of servers and network specific devices,” Evans says. “Attention is shifting toward protecting the most critical business assets or processes rather than buying groovy cyber technology.”

Awareness programs at not only the individual level, but a governance level, are fundamental to the design of an all-inclusive security strategy, Winkler says. “An awareness program has to be comprehensive and multi-modal. You have to try to impact people by having a ubiquitous program that constantly reinforces good security practices.”

Designing a multi-tiered, full-coverage cyber security program has a set of basic requirements: human awareness at every corporate level, effective technological infrastructure, legal security in case of liability and the educated governance to organize and implement a strategy balancing those factors.

A New Approach

From a management standpoint, the adoption of top-down security approaches is the first step in waging a war on cyber criminals. Recognizing senior-level influence is a relatively new development in cyber security. “We have seen the creation of the Chief Privacy Officer in the last decade, where that previously didn’t exist,” Blair says. The most important and difficult part of innovation within a business, he continues, is “adjusting corporate governance practices around any new or evolving issue.”

The development of new technologies (AI, the cloud, intrusion detection systems, advanced firewalls, etc.) paired with a modern top-down talent approach create an effective dichotomy with which to deter cyber criminals both proactively
Christopher P. Skroupa is the founder and CEO of Skytop Strategies, a global organizer of conferences. GCSEC is supporting Skytop Strategies for the event "GLOBAL CYBER SECURITY SUMMIT - DEVELOPING A ROBUST CYBER DEFENSE STRATEGY" - [http://goo.gl/ExmIHo](http://goo.gl/ExmIHo)

Article: [http://goo.gl/h03ExW](http://goo.gl/h03ExW)

"Global" is not the title of a book (will release Palinesto publisher) but the beginning of a new challenge for Roberto Panzarani, just back from a trip to Brazil. Ten years ago has been published the essay "Viaggio delle Idee" (Journey of Ideas - Franco Angeli translated into Portuguese and disseminated throughout Brazil), a prophetic essay in which the researcher draws attention on the complex dualism between ICT and social-politics contest already unable to give more space to the intellectual capital as the real engine of neo-capitalism.

In spite of the past, in this context it is crucial the combination between persons and tools, including our ability to manage the change and progress of scientific and technological research.

Professor, the innovation does not stop but yet there are rigid and unchangeable constants such as our persistent inadequacy in the understanding of innovation processes at all levels. "Global" analyses this cognitive deficit, what are the conclusions? The reflection on the development paths of management of innovation has been and continues to be the North Star of my activities of teaching and organizational studies. In this work I focus on two important factors of innovation: technology and globalization. In the last trilogy (sense of community, business collaboration, Humanity editor's note) I was focused on technological factors that were changing the face of companies’ business and the same rules of the economy. Now, in the middle of the discussion I placed the second factor, the globalization.

Globalization has showed signs of weakness in these years, do not you think? There isn’t single answer. It should be noted that we have gone through various globalizations. From "homo Naledi", nomadic by definition, to the discover of the "new world", industrial and post-industrial. Today we talk of the networks globalized, thanks to the diffusion of technologies and devices.

What are the consequences of this dynamics that impact on socio – economic changes? Simple: we are not faced with an incremental innovation but with a disruptive innovation, which obliges us to continuously update. In the previous "globalizations" the times of innovation diffusion were slow, now within a few months the change invades our daily lives, as well as the markets recording the continuous invasion of increasingly aggressive competitors who come from distant worlds. In this context the our neural synapses are urged constantly to revise and understand the reality. This operation is not easy and exposes a paradox...

Which? The Indian anthropologist Appadurai explains it very well: "We live in a world characterized by an increasing gap between the globalization of knowledge and understanding of globalization, at the same time the knowledge of the world is increasingly important for anyone while the opportunities to acquire this knowledge are shrinking". The thing, however, more difficult to accept is that the phenomenon denounced by Appadurai is not happening only in developing countries but also in the countries of the old continent, real enigma of globalization.

Are you describing a profile of the European crisis? Yes, one of the profiles, maybe the most disturbing. While in the phase of the Columbian Exchange, the knowledge was at the center of "discover" and conquest, at this historic moment the Europe behaviour was not many knowledgeable. It will be difficult to recover, as it will be for Italy. A fact for all: 45% of the students have abandoned our University in 2013, it was the highest number of the Continent. In these conditions, it becomes impossible to activate a governance of globalization. The most capable countries to invest in knowledge and assets will be the winners of the match.
There is no reason to be happy. Under these conditions the colonizing Europe may be dominated by other regions of the world. An unexpected but possible scenario. What do you think about that?

As claimed by Alec Ross in "Il nostro Futuro" ("Our Future" release Feltrinelli publisher) a big part of the business is moving to Silicon Valley, which has become rich like the ancient Rome because collects “tributes from all its provinces”. Platforms like Uber and Airbnb have flipped the system balances. The same thing for the economic ads that by now we can find on Google advertisements. In a nutshell, globalization has transformed in the empire of knowledge and will need more and more of expertise to be managed and controlled.

Well, we have described the shadows and contradictions. Is there any light in this change?
Fortunately, we can see processes of self-organization and continuous adaptation in different contexts. The world is more and more little and interconnected in these regions “far from the balance”. To use a thermodynamic metaphor, it experiences organizational forms, collaborative moments and phases of exchanges and discussion on the threshold of uncertainty between the cosmos and chaos. In these topics, we are reinventing the company and the same business foundations.

An important section of your research concerns the specific cases of social innovation. What is it about?
This is the most authentic and vital part of the essay, is the part of globalization with which we measure ourselves. I think about Chile that has decided to attract young people to create new high-tech companies or about the government of Argentina that invests in know how and intelligence. We should follow the virtuous example of these countries without fear and prejudices due to old logics.

It will not be easy to fill this gap of culture and vision. Don’t you believe that we have failed too many times?
We have not other choice. “Global” describes the changing world through stories that give a different “colour” of the globalization that is not an abstract phenomenon. It is life itself that goes beyond the traditional fences, turning to open networks, real and virtual. People are desirous to "create" a better world, in which human development and economic progress will eventually converge.