Staying Ahead in the Cyber Security Game

What Matters Now

Erik van Ommeren
Martin Borrett
Marinus Kuivenhoven

Co-written with IBM

Premier Business Partner IBM

SOGETI

Staying Ahead in the Cyber Security Game

What Matters Now

Erik van Ommeren Sogeti
Martin Borrett IBM
Marinus Kuivenhoven Sogeti

2014
Sogeti and IBM

1st Edition, April 2014
© 2014 Sogeti and IBM
Book production LINE UP boek en media bv, Groningen, the Netherlands
ISBN 978 90 75414 77 6 (book), 978 90 75414 78 3 (eBook)

Table of Contents

IBM Foreword — A Changing Landscape

By Steve Mills

Over the last thirty years I have been fortunate enough to play a role in shaping the way that technology impacts business and industry. Today, IT systems have changed the way companies deliver products and services, how people communicate with one another, how organizations make decisions and even the way individuals understand and interact with the world around them.

Many of these changes are being driven by the confluence of significant, interrelated trends around cloud, mobile, big data and social networking. While each of these shifts is independently significant, taken in combination the pace at which our relationship to IT is changing is extremely rapid and equally impactful.

However, just as these shifts have pervasive organizational impact, the emergence of organized crime, state-sponsored attacks and social activism in the digital world all speak to a new reality in which security risks cannot be adequately understood as merely IT challenges. These issues can often threaten an organization's brand, intellectual property, sensitive business data and financial resources.

The presence of these risks is changing the way many organizations approach security. Chief Information Security Officers (CISOs) are now accountable to the CEO and the Board and have assumed the role of translator between business leaders and security experts, helping each group to understand the perspective, challenges, requirements and objectives of the other. This is

a critical partnership for both organizations as it helps security teams to develop a more nuanced understanding of business strategy versus IT risk and allows business leaders to not only make more informed decisions about budget and personnel, but also provide their support in driving enterprise security transformation.

There are important security considerations associated with how technology, and by extension, the world, is changing. There are ongoing, substantive debates about privacy, the role of government and how new computing models impact security considerations. While this book will explore many of those topics in more detail, it is also important to note the unique opportunity that exists at this moment as well.

While cloud, mobile and big data are often cited as security challenges in the context of data storage, device management and privacy, each one of these shifts presents opportunity as well. Cloud technology can be used to rapidly deliver security and threat intelligence to endpoints around the world. Mobile devices and the applications on them have the potential to be more secure than traditional laptops. Finally, many organizations now see literally billions of security events every day and the ability to apply advanced analytics to this data provides organizations with the capacity to detect and respond to threats in a way that was never previously possible.

Unlike previous changes in IT, these shifts are occurring at a time when organizations are more cognizant of the risks than ever. While security teams will now have the opportunity, and mandate, to embed security into the technology and business process of the organization in a way they never have, they will also be asked to deliver better results in the face of skills shortages and pervasive technical complexity.

Security teams will play a critical role in enterprise transformation, but their success will be predicated on their ability to integrate controls and processes and simultaneously develop new practices around the increasingly important fields of analytics, intelligence and incident response.

Steve Mills
Senior Vice President and Group Executive,
IBM Software & Systems

Sogeti Foreword — The Game is On

By Hans van Waayenburg

Sending an email, making a bank transfer, ordering something online or booking your flight directly on your mobile has never been as easy and fast as today. About 50 billion devices will be connected to the Internet in 2020, most of them barely protected, a fact that implies as many potential doors for hackers to intrude in our devices, our companies, our homes and personal lives.

Today, the increase of networking and connectivity enable our organizations to become more efficient, more productive and better informed. Data and Information access are key assets for every individual, every company and every state. Thus, Information Technology has become vital for decision-making. It allows process optimization and industrialization of anything ranging from railway track switching, to air traffic control, from gas and electricity distribution to chlorinating our water supply. However the current, ever increasing, adoption of digital technology has been accompanied with a lack of understanding of the consequential stakes, especially amongst the young generations. *"We don't care how it works, as long as it works."* Therefore, we have become vulnerable.

At first, computer hacking was a game, a playful hobby for a few curious, skilled people. As the Internet evolved, these skills became a political or ideological tool in the hands of hacktivist groups who perceived their activity as a legitimate form of social protest. Equally disturbing is the criminal use of networks and technologies, with many organizations seeing literally billions

of events every day, plenty of which include significant security threats targeting customer data, intellectual property and confidential data. Cyber espionage, targeted against both government and industry, has become a common practice.

The borders between all of these security threats are fuzzy, in part due to the design and topology of cyberspace: the boundaries between thief, spy and activist are a lot less clear than in real life. And though there are some regulations that rule the web, a large grey area still remains where well-organized attackers can operate with seeming impunity. Cyberspace provides the perfect cover making these actors very hard to detect and identify. Further, the complexity of cyber attacks makes it even more confusing. There are no flags, no uniforms and no established, understood rules of engagement.

A piece of malware, Trojan or a worm could remain dormant in an IT system for months before being detected, meanwhile tapping into your information. Each night, thousands of gigabytes of technological and strategic data are stolen from thousand of computers of our Western companies. A cyber attack can cause significant damage at a very large scale, for long periods of time and at low costs.

Finally, a cyber attack is usually not claimed as stealth and anonymity are clear benefits of choosing to operate on the Internet. Identifying the guilty remains highly complex and depends on few characteristics like concordant items of evidence, the language used, the names of commands and so forth.

One of the main issues of cyber incidents is the breach of trust in our IT systems. Attempts have even been made to compromise SCADA systems and the impact of these threats carry serious potential consequences. Already the "simple" hacking of a bank, the social security system or any other strategic infrastructure

or service would cause a huge breach of trust from consumers, users and citizens. Taking into account our ever-increasing use of technology, amounting to technology dependence in every aspect of our economic and social environment, our world is far more vulnerable than we might think. The threat of a global breach of trust requires constant diligence and awareness in order to be mitigated and ideally prevented.

This urgently calls for *Staying ahead in the Cyber Security Game.* For now, these threats cannot be suppressed but we can contain them. We must keep playing this chess-like game and balance it in our favor. I hope this book, which I am glad to have coproduced with our trusted partner, IBM, offers you both an increased appreciation of these issues as well as ideas to help you stay ahead of the threats facing your organization. In the face of this challenge, it is critical that we combine forces, not only between service providers but also public authorities, in order to keep up and always be one step ahead!

Hans van Waayenburg
Chief Executive Officer, Sogeti

Executive Summary

Cyber security is center stage in the world today, thanks to almost continuous revelations about incidents and breaches. In this context of unpredictability and insecurity, organizations are redefining their approach to security, trying to find the balance between risk, innovation and cost. At the same time, the field of cyber security is undergoing many dramatic changes, demanding organizations embrace new practices and skill sets.

Cyber security risk is now squarely a business risk – dropping the ball on security can threaten an organization's future – yet many organizations continue to manage and understand cyber security in the context of the IT department. This has to change.

Technology is continuously changing and there is no recent shift larger than the explosion of mobile device usage. People bringing their own devices to work is an unstoppable wave engulfing organizations, regardless of policy. The demand for BYOD is surging, but it poses serious challenges for how security is managed, both in terms of technology as well as process and policy. These mobile devices seem to be the antithesis of everything security professionals have been trying to do to keep things secure: they are mobile, rich in data, easy to lose and connected to all kinds of systems with insufficient security measures embedded.

Technology also brings opportunities, for example, big data offers the promise of new insights that enables a more pro-active security approach, provided organizations can employ the people who actually understand this new technology.

Most focus on state of the art security revolves around people and their behavior. It is common understanding that with enough determination and skill, a persistent attacker will eventually be able to break any defense, but making this process difficult every step of the way lowers risk and increases not only the time in which organizations can respond to incidents, but also improves the ability to intercept them before the impact becomes substantive.

In order to do security right, it has to be made part of the most elementary fiber of the organization, both in technology – including security as part of the design – as well as in behavior – giving people secure options that they prefer over less secure ones. Simply using fear as a tool to motivate people is going blunt very rapidly.

1
Staying ahead in the Cyber Security Game

What matters now

Cyber security is a set of people, process and technical practices aimed at protecting critical infrastructures, digital business and sensitive information from internal and external threats or negligence. It is a field that is continuously in motion, perhaps even more than IT itself. Still, the essence remains to guard the qualities of IT that make it the reliable resource that business and society has come to depend on: confidentiality, integrity and availability. But what are these changes that the industry is experiencing today? What matters now? The themes that we discuss can be categorized in these grand questions:

1. Can we trust the system?

The biggest discussion of today is a fundamental question about the reliability and security of the Internet and perhaps technology as a whole. The Internet was never designed with security in mind and today it is very clear that it's possible to compromise almost anything a dedicated hacker sets his mind to. Security and trust are now center stage in the public debate. This is triggering new research and innovation to make the Internet a more secure infrastructure.

2. Can we make the organizations more secure?

The next level down is about creating a secure organization that can survive and thrive in the midst of imperfect technologies. To achieve this, to build a security culture in the company, the conversation has to pivot from fear to value. As threats become more sophisticated and targeted, and their associated impact on organizations becomes increasingly significant, security must evolve from focusing on fear and risk to an understanding that establishing and maintaining trust and confidence can, and will be, a competitive differentiator across industry and government. Security is no longer an IT risk, but an enterprise business risk, so it must be managed accordingly. In addition, it has become both accepted and widely understood that attacks and incidents are questions of "if" not "when," and as a result, practices associated with detection and response must be an essential, multi-disciplinary part of any organization's security strategy.

3. Can our people win the game?

Right now, the reality is that sophisticated attackers are breaking through conventional safeguards every day. They have a number of strategic advantages over those tasked with defending networks, namely the element of surprise, the ability to research and target specific, unsuspecting individuals, infrastructure complexity and a global cyber security workforce that is already stretched thin. The general population is not composed of security experts and the imbalance of expertise on each end of a spear phishing email is a significant strategic and tactical advantage for attackers. For security professionals to address these concerns involves a combination of more robust skills develop programs, infrastructure simplification, more advanced analysis and response capabilities as well as user education and empowerment.

4. What will technology bring next?

In one study, 70% of security executives expressed concern about cloud and mobile security. These IT shifts challenge conventional security models and require not only new technology, processes and policy, but significant culture change associated with the nature of control. However, these changes also provide new opportunities as well. Secure-by-design principles, which have been developed from years of experience, can be applied at the onset of new projects and deployments. Cloud offers new delivery models for security and threat intelligence, big data and analytics offer the promise of changing the IT security industry in the same way that business and industry now rely on data and the associated analysis to understand trends and make decisions.

Ultimately, the cyber security game will not have an end, and there will be no definite winners and losers, but that end can be replaced with the persistent pursuit of strategic advantage, a rebalancing of the equation between attacker and defender. By combining forces, by taking time to reflect and consider what is really happening and by diligently applying what we have and know, organizations *can* get ahead, which is as close to winning as exists in this industry.

About this publication

This book aims to inspire and provoke new thoughts and insights, even if you are familiar with the topic. For people new to security, it's a primer to get an idea of what matters today. We've purposely chosen to be brief and focus on the most recent and relevant topics. You will therefore not find extensive descriptions of well-known practices such as how to practice security risk management or how to build an authentication model, even if they are still important today. Also, we've decided to look at the organi-

zational, management and governance dimensions of security, staying away from technical discussion.

The book can be of course be read cover to cover, but is also structured to lend itself to reading just the chapters that are of special interest to the reader. After the introduction, each chapter highlights one of the most recent developments, what it means and what you should consider doing differently as a result.

Acknowledgements

Many people have contributed their insights and ideas to this book. Through workshops, interviews, anecdotes, written contributions and reviews they helped zoom in on the most relevant and interesting developments related to information security today. The authors would particularly like to thank the customers who took time to talk to us about their vision, challenges and solutions. You will find some of their (anonymized) quotes throughout this book.

We'd also like to thank these people for their contributions, in alphabetical order: Rogier van Agt, Didier Appell, Jean-Michel Bertheaud, Jean-Marc Bianchini, Jaap Bloem, Michiel Boreel, Bryan Casey, Jeff Crume, Doug Davidson, Vijay Dheap, Menno van Doorn, Jean-Marc Gaultier, Stéphane Janichewski, Edouard Jeansson, Yves Lefloch, Arnauld Mascret, Véronique Mireau, Patrick Morley, Charles Palmer, Orion Ragozin, Patrick Recchia, Pierre-Luc Refalo, Djaafar Senoussi, Rene Speelman, Mike Turner, Martin Visser, Charlie Weibel-Charvet, Jim Whitmore.

2
Security Center Stage

How the continuing battle between the "good guys" and the "bad guys" is ultimately making the world more secure

Where would the world be without the Internet? The network of networks, which was created to be a simple, resilient communications channel that could survive even while experiencing large-scale network disruptions, has defined our present era. Initially the Internet was just a text-based network, but over time graphics, then commerce, streaming video and many other extensions have been bolted on. And now (finally) the time has come to seriously think about security and privacy.

> *"Today we do not know how to legally pursue cyber-criminality in the national or global legal framework. Which framework will have the authority? Who will be the cyber police? Is Interpol the right agency? Is activism a form of cyber criminality? Some say that I am a terrorist. I think I'm more a kind of counter-force. I do nothing but trying make myself useful!"*
>
> – Cyber activist

It's not that security has been completely absent all this time, but the increase in both our dependence on digital communications and the level and number of attacks have taken it center stage. Since the early days of e-commerce, the merchants and credit-

card companies have been fighting to maintain the integrity of online payments. But today is different: it is no longer just money or personal credit card information that attackers are after, it's much more. The reputation and livelihood of entire companies are at stake. For any decent size company, a serious attack with malicious intent could mean serious business disruption.

Attackers today are diverse and dynamic: there are international criminal gangs, state sponsored actors, idealistic cyber activists (*hacktivists*), and insiders ready to leak information. These attackers present the ultimate nightmare for any security officer. Advanced Persistent Threats have emerged where very capable individuals are absolutely determined to break through defenses and will try anything they can to achieve their goal. Full proof defense against these advanced threats has proven virtually impossible and any defense demands an approach that is different from the regular, cross the board and generic security measures. It will encompass everything from good governance, real-time detection of ongoing attacks, smart security systems, training people, reviewing data architecture, setting up response mechanisms, reviewing the interaction with partners and rethinking existing processes in IT and business. To remain resilient, with every new technology project, security should be considered from the start. But still, a certain resignation has spread among security experts, leading to a sort of *un*conventional wisdom:

> "There are two types of companies: those who have been hacked and know it and those who have been hacked and don't know it." [1]

> "Keeping the flow of information running freely is an economic imperative."
>
> – The Cyber Security Manifesto

1 http://www.usatoday.com/story/cybertruth/2013/09/26/lexisnexis-dunn--bradstreet-altegrity-hacked/2878769/

Privacy and security are two sides of the same medal

In the wake of big data, social media and increased availability of location data, privacy advocates have raised questions about who owns data (or "metadata") and what control both individuals and organizations have.

Many of these questions have yet to be answered from both a technical perspective (what tools can be used?) as well as a financial and societal view. Ultimately, privacy is both a cultural and a personal issue, and a space where the perspective and impact of digital natives is increasingly significant. Raised on the Internet, this generation brings new views on privacy and ownership of data.

There are some emerging concepts surrounding data ownership that would upend existing practices. For example, one idea is centered on the concept that any data about a person will eternally stay within the control of that person. Any company that would like to use the data would have to negotiate with the owner for access and use. This would only work with a complicated system of authorization and access models and the reality with most of these concepts is that they would only work if universally adopted. This is also a similarity between privacy and security: it extends organizational boundaries. Once a company has established its own privacy and security culture, it needs to share it with their customers, partners, government, and public agencies.

On the backend, there are also similarities in how companies should deal with both security and privacy. For example, if data isn't needed, it should be deleted in order to effectively reduce both security and privacy risks.

The impact of cyber security... does it matter?

In the end, how does all this affect organizations? Does it matter what the ideological background is of someone who attacks? Does it matter that some of the attackers may be state sponsored? There are important considerations here, such as resources available to the attacker and how organizations could ask government for support if foreign involvement is detected. However, while risks will vary in both nature and severity depending on industry, the reality is that when an attack is on, an attack is an attack. Organizations would only care about the intent of the attacker so far as to define the intended harm the attacker has in mind. Is the objective to deface a website, steal secrets or disrupt business? The ideological motivation or sponsorship is at that point of lesser interest.

In the variety of actors on the attack side, state sponsored attackers may represent the top of the line. Yet criminals, who can be anywhere in the world, are not far behind, using the exact same exploits and security holes.

The least skilled participants in this dynamic are the regular users, users who inadvertently post sensitive data online, easily give up their password in response to a malicious email, share their password with a friend at work or leave a thumb-drive behind in their rental car. This category of users is one of the most significant challenges for Chief Security Officers today. They must come up with a strategy and approach to both put adequate controls around these individuals while simultaneously not impeding on creativity and business outcomes.

A wish list for cyber security

During a recent event, an international group of Chief Security Officers listed their wish list for the near future, answering the question "What should be the most important advances in security on the coming few years?" These were their top answers, which fall into three categories:

Better solutions for securing end-to-end communication

- To have better authentication mechanisms by which you can be 100% certain about who is connecting to a system.
- To be able to use secure applications over an insecure infrastructure. Acknowledging that PCs, tablets, phones and the Internet itself will never be secure, it is imperative to build secure applications on top of this insecurity.
- An increased role for biometrics, which could support authentication online, enabling new levels of security. This includes fingerprints, blood analysis, DNA sampling, heartbeat and other biomarkers.

Smarter systems

- To have a self-learning security system: a system that could learn from day to day operation and which would automatically block all unusual movement in your systems.
- Auto classification of data, automatically finding which data is worth securing.

A better way to communicate to users about security

- To have a framework of security warnings and alerts that will help the user better understand the security risk and implications of certain actions. This could apply anywhere from an app store to certain actions inside a corporate system.
- A label to put on applications and certification for devices that would inform people of the level of security that is provided.

Wishful Thinking by the Chief Security Officer

It's no surprise that Security Officers are stressed. Their industry is one where a 100% guarantee can never be offered, the risks are ever increasing and budgets remain tight. Some people say about security: "*you just keep iterating until time or money runs out,*" which is a highly unsatisfactory approach. Yes, organizations will need a strategy and yes, there are plenty of tools and industry standards to pick from, but there is no certainty that the newest and most powerful attacks have yet to be discovered and documented.

> *"It is no longer major figures getting attacked. Today, attacking SMEs is a godsend for hackers."*
>
> – CISO at a financial services company

So what would change the game? How could the world of security make some serious strides? There are some basic realities that will probably never change, such as that the Internet will always be an insecure infrastructure, or that organizations will never have enough budget, people or time to address all vulnerabilities, or that one can never truly *prove* that the right decisions have been made. Yet, there is hope: the increased awareness among executives and advances in technology or international law enforcement may change the game for good.

> *"The first things to do are to rely on good practices, watching the market for references, standards. I'm surprised that there aren't more forums (...) to share good practices."*
>
> – CISO at a manufacturing company

An important emerging opportunity is centered on smarter systems that adapt and learn. There are a lot of developments in

this area, but predicting the future remains a challenge because ultimately it involves trying to predict human behavior. The first time something new happens it will by definition not be known by the security system. Organizations and the people within them are constantly changing so the ability to distinguish natural business process evolution from a potential security incident remains a challenge despite the significant progress that has been made in the area of security analytics.

It has been said that the next era of IT will be centered on "cognitive computing," or systems that naturally learn from their environment. This is the step that ultimately goes beyond simple rule, or even principle based analytics capabilities.

While it may be years for such capabilities to become common in the market or in security environments, there are steps organizations can take now to begin preparing for, and taking advantage of this shift, namely in how they evaluate and cultivate skills within their organization. As data and analytics become increasingly central to how organizations identify and respond to security threats, organizations need a different type of security professional, people with a combination of security and data analysis expertise.

Building practices and expertise around analyzing security telemetry is both an immediate value add and a key element of building a long-term security strategy.

The good that will come from all this

While it is sometimes difficult to view the constant barrage of disclosures, threats and breaches as a positive, there are two very tangibles outcomes that are largely positive. First, as most attacks today involve targeting individuals, increasing public awareness about security threats will ultimately make individuals more resil-

ient to attack. The more security is discussed in the public realm, not only do people understand that there is a significant threat, but there is more discussion about the nature of the threat, the tactics that are used in attacks and key steps users must take in order to protect both themselves and their organizations.

> *"What I find interesting today is that at the State level cyber security and cybercrime are truly taken into account. (...) The foundations have been laid and we must make progress in this area."*
>
> – Army chief of information security and cyber warfare

Secondly, the increased focus and public dialogue on security issues is forcing the creation of more resilient IT infrastructure. In the absence of public pressure and accountability, many security issues would go unresolved due to the lack of a forcing mechanism. Many organizations have historically approached security as an afterthought, and, even worse, only addressed issues after an incident had already occurred. However, today the public pressure, awareness and understood impact of security threats is causing organizations to consider security as an essential element of how products and services are designed and delivered, how business processes within an organization are structured and how both customer and confidential data and information are stored and protected.

As security becomes more important and better understood, it will ultimately become increasingly difficult to exploit both human and technical vulnerabilities for illicit gain.

> "Access to an Open Internet is a fundamental human right."
>
> – The Cyber Security Manifesto

3
Curing the hangover from the Bring-Your-Own-Device party

Widely available devices and services will flood the organization

"With BYOD we are left with a major security issue, because it creates gaps in the IT of the company. This did not exist ten years ago, and it is for me the real challenge for the coming years."

– Army chief of information security and cyber warfare

The relation between people and their gadgets is more intimate than ever. Personal preference, work-style and "feel" determine which device is best for someone. People are taking their "personal" devices to work and use them there. No longer can the corporation really decide which laptops, phone, tablets, or phablets are used for work. For now, many organizations still try to stem the flood of personal devices through strict polities forbidding every personal device, but in the long run this might well prove untenable. Other companies are trying to formulate Bring-Your-Own-Device policies – or more often Choose-your-own-device policies – that support the desire to use the device of your preference, while maintaining corporate security. This is much harder than it seems. Could BYOD be indicative of the end of proper control over devices and technology?

"Companies no longer control their software and hardware environments."

– The Cyber Security Manifesto

What is recent?

"We cannot block the arrival of new technologies. We are forced to adapt."

– CISO at a manufacturing company

BYOD is top of mind for many CIOs and even expanding into BYO-IT: it's no longer only about the devices, but also about the services consumed on the devices that are widely available "in the cloud." Employees bring anything from phones and tablets to collaboration, file-sharing and complete CRM solutions into the organization. The marriage of consumer devices and cloud services has resulted in enterprise-grade features that are highly usable in a corporate setting.

Why is this relevant?

Traditionally, defending the perimeter was the main or only line of defense. Letting other devices or even services in has upended this paradigm, forcing us to rethink the security of the entire technology portfolio.

What new action should I take?

The main issue with BYOD is that most backend systems are not designed with this kind of flexibility in mind and the change from the perimeter model to a new cross-layer model of security is quite radical. The model itself may be familiar for a little while

now, but implementing it across an organization is still a large step. It encompasses these kinds of actions:

> *"However, the attitude of some managers can be annoying. Some do not show by example. It is very often related to the person. Some higher-ups are aware of the risks and make it a priority for the company. But it is still too little."*
>
> – Army chief of information security and cyber warfare

- Implement security across the entire technology stack. No longer can we inherently trust a single device, channel or application: at every step of the way we have to verify that an authorized user, for a recognized goal, initiated the requested interaction. This means that any technical component, from the enterprise service bus to the web server and the database must have some form of authorization model built in that relies on "whitelisted" actions: define what is allowed and disallow anything else. Here you will have to sacrifice some IT flexibility (generic, open interfaces) for security (specific, closed interfaces).
- Security is about data, or more precisely about data and context. The authorization models should not be based on "access" (login to the system), but on access to the data in combination with context or scenarios: can this user, at this time of day, at this location, through this device, for this purpose have access to this functionality using this specific data.
- Need for a strong identity check: an integrated user model is a basic premise for any security approach, but in today's reality, the identity model should include a personalized security model, defining what kind of behavior is "normal" for a certain user, much like credit-card companies do to detect fraudulent behavior.
- Transform the perimeter model into a layered or onion model: it's no longer about "inside" and "outside," but there are probably several layers in between. The goal should be to define an area as small as possible that is truly "secret" and ever expanding

areas where data is less and less restricted. The more "secret" the layer you are trying to access, the higher the demands regarding authorization, device, network used, encryption etc. "Secrecy" in this context translates to the damage that could result from exposure or disruption of that data: what would happen when your IP gets stolen, your customer data is exposed or your strategic plans are shared with competitors?

- Don't forget the old model: while addressing all things mentioned above, the perimeter is still an important layer of defense, hence the attention to device management, virtual machines, split-memory devices etc. One of the challenges of the modern IT infrastructure is the multitude of possible combinations between devices, networks, applications and messaging structures. Any of these elements could be the weak spot, so for any known element in your infrastructure, there should be a focused and targeted security solution. It should be very clear which devices are not under total company control and should therefore not be trusted, even if an optional security solution may be deployed.
- Finally, of course there are the legal and financial aspects of BYOD: create clear policies that spell out who will pay for the device, who is responsible, what security protocols must be followed, when the company can access the device, and what kind of liability is accepted.

Universities serve as great role models of how the ultimate BYOD could work: all students, and often the professors too, carry their own devices and need access to all kinds of tools and systems. They bring their own devices and often choose their own tools to work and collaborate. Conceptually, this could work for other organizations as well. And, coincidentally, the same security models would also fit with other important trends relating to network organizations, supply chain integration and project alliances. Alas, for now the infrastructure and backend systems are not ready for this. So while BYOD may be the ultimate desire of employees, Choose-Your-Own-Device (CYOD) is often the best we can do for now.

4
With the enterprise at risk, don't leave security to IT

Mitigations should include enterprise level mitigation, not just the IT approach

In present day organizations, Information Technology has taken center stage. IT lies underneath all processes, it enables many of our business models and it is in the center of engagement, experience economy and customer intimacy. Our dependence on technology is larger than ever before, not just to record or process orders but everything from marketing to sales, delivery, service and all internal processes. The potential damage of system outage or, even worse, system sabotage is larger than ever. Still, managing the IT security risk and preparing the response to incidents is often delegated to the IT department, even while the impact is now so much broader. This has to change.

> "Security governance cannot remain a minor concern now that cyber security is a major concern."
>
> – The Cyber Security Manifesto

What is recent?

In the past few years, companies have realized how important IT is for their customer interactions, their core processes. Spurred on by the emergence of mobile apps, "social" software and "Systems of Engagement,"[1] the level of IT dependence has increased greatly in many new areas of business. Meanwhile, there have been high profile IT failures which have brought further awareness to our IT dependence, such as an airline that stranded its passengers because of system failure, innocent people who were arrested because of system errors[2] or even problems with US elections and stock markets[3]. The volatility of this risk has increased dramatically: the knowledge about exploits spreads extremely fast and there is a working market to buy and sell zero day exploits – the exploits that nobody else is aware of just yet. The effect is that today the time between "it can never happen" to "serious risk" is shorter than ever before.

Why is this relevant?

The response to an incident determines for a large part the damage that will be done to your customers, your reputation and your ongoing business. The right preparation can accelerate the response, or even mitigate the business risks before they occur. Enterprise risks should be countered by enterprise level mitigation.

1 http://www.wikipedia.com/SystemsofEngagement
2 http://mybroadband.co.za/news/software/39959-high-profile-software-failures-of-2011.html
3 http://www.net-security.org/secworld.php?id=14142

What new actions should I take?

In the traditional view, it's primarily the IT department that prepares for and acts on incidents: closing the holes, shutting down systems, recovering lost data and perhaps tracing an attacker. Only then would other parts of the organization wake up and start to get involved, if at all. Managing the risk from an enterprise perspective changes the level of preparation and response:

> *"Whenever there is an attack, in my opinion, the best method is to not react immediately, and think first."*
>
> – CISO at a bank

- To create a security strategy, the organization reviews the business risks associated with technology failure and attacks. It plans for mitigation of these risks in the technology space (strengthening defenses) but also – especially – in the organizational domain (for example by adjusting terms and conditions to minimize liability, educating customers on what to do when something happens, preparing communications, preparing an escalation protocol, aligning partners, etc.). These activities also include efforts to minimize business risk from internal leaks or attacks by designing a different segmentation of work, changing review procedures and other provisions that lower the chance and impact of data breaches or sabotage.
- The incident response plan must contain details on when and how to communicate to the public about security incidents. Depending on the severity of the incident, different types of messaging can be developed, but for any incident there should be a single and coherent message for both internal and external communications. The primary goal is to protect customers' interests and reduce their uncertainty. Communication has to be fast and effective and parties such as law enforcement

authorities, regulatory agencies and partners must be informed when appropriate.

- Build a multi-functional response team: IT in collaboration with communications, legal, senior decision makers and other relevant business experts. This has been recommended practice for a while but still isn't done often enough.
- Test and practice the emergency response with the team, so they know each other and know the procedures. As one security consultant phrased it: "If there is an attack, do they know how to react, or otherwise know who to contact? Managing incidents should be simple and clear. If they need a manual, it will not work."

> "Responses to emergency cyber security issues have to be well prepared, well oiled and well exercised."
>
> – The Cyber Security Manifesto

In organizations today, the role of CIO is increasingly filled by someone with a business background, to make sure that IT is run a part of the business and not as a semi-separate entity. Similarly, the CSO or CISO should have a strong business network and focus on elevating the security discussion to the right level. Inject information security risks into the enterprise risk management considerations and, most important of all, help minimize the business risk of technology failure. The challenge is to spend time on this, while at the same time not dropping the ball on the operational part of the job, of course.

5
Security is already created or lost at the design stage

Privacy, quality and security all need to be applied from the start

If only we could redesign everything from the start, then it would be easy: we would simply apply all best practices we know and then the data and systems would remain secure. If only we could? The notion of security-by-design sounds simple and highly desirable: we design the system from the ground up on secure principles that are strong enough to be resilient against all future threats. For any new development, it is indeed that "simple:" security-by-design means designing security into a system right from the start. For existing software, this opportunity has passed, but even there it can be worked in by making sure any new modification makes the system more secure in whatever way possible. "Whenever you plan a new release for this older system, you HAVE to apply a new security pattern."

What is recent?

Software development has professionalized dramatically in the past decade, with more emphasis on modeling, agile methodologies, code generation and better use of frameworks, components

and partial solutions. It means that the code creation process has become much more predictable and controllable, and that security patterns and components are widely available. With the introduction of Cloud, a big transformation is happening in IT, where homegrown systems are being replaced by commodity systems, or where new solutions are being created specifically for this new environment. A great opportunity to now "do it right!"

> *"Security must be at the heart of systems, with Trusted Computing. There is a great need to build secure applications within an infrastructure that is not! We will never secure the entire chain. Security should be first in the planning of the projects, before thinking of the rest. More often it happens the other way around."*
>
> – CSO of a research institute

Why is this relevant?

Security-by-design is one of the powerful approaches we have available to make *everything* more secure. Not using it is leaving a big opportunity on the table. With product vendors very aware of security risks, custom development is one of the most important places where vulnerabilities are introduced into your technology infrastructure. Putting security into every layer is the only way to be both resilient against attacks and be as future-proof as possible – for example being ready for new channels, new connections, new integrations, because the core system has security woven in throughout.

What new action should I take?

In the software testing world and the privacy debate, we've learned that the earlier in the process you take certain requirements into account, the cheaper it is and the easier to implement. The same goes for security:

- Make security a part of the Enterprise Architecture discussion, with strong requirements about data, verification of authentication and by default not "trusting" other components or layers of your architecture. Establish an Enterprise Architecture process that is empowered and supportive in helping project teams make the right decisions.
- Create anti-patterns: negative use cases that describe the undesired behavior too, so that it's clear what should be built and tested along the way. For example when a genuine use case reads "An authenticated user can read his own latest five transactions," you can turn that into the undesired situations of "A NON-authenticated user can read every latest five transactions" or "An authenticated user reads SOMEONE ELSE's latest five transactions." This helps to make clear what the underlying code should and should not allow, all the way to the data level. It establishes very early on in the design process where the restrictions should be built in.
- Put enough time and budget into your projects to address all non-functional requirements right from the start: security, privacy, quality, usability, manageability, etc.

> *"Today is worrying. The perimeter of the network has disappeared. We had a fortress, which disappeared gradually as the network expanded. How to secure data in this changing context?"*
>
> – CISO of an educational institution

How to proceed?

Security-by-design starts when a development team acknowledges that there are circumstances when bad things can happen to seemingly good software. From that admission, it flows that design necessarily involves satisfying a combination of: functional requirements, non-functional requirements and assurance (or risk avoidance) requirements. Given three requirements, one in each category, it is critical to know how stakeholder and end users would prioritize the requirements. In years past, the priority might be ranked as: function (productivity oriented), non-functional (look and feel oriented) and assurance (especially if it affects productivity or look and feel). In today's world, we have evidence that the priority is different, that more often assurance overrules functional or non-functional requirements – for all the right or wrong reasons.

Security-by-design proceeds along two parallel paths. One is the technical path, where risk avoidance/assurance requirements are documented. The other is the project management or process path, where the decisions about resolution of these requirements are tracked to satisfactory resolution.

> *"Security is integrated at the start of projects, which wasn't the case 10 years ago."*
>
> – Army chief of information security and cyber warfare

What are the challenges?

The ability to orchestrate and control projects is one of the biggest challenges to security-by-design. All software development projects face challenges from budget, schedule, resources, complexity as well as changing requirements and priorities. While it is well known that the absence of a security-by-design approach

can have severe impact on schedule, resources and complexity of project, there is also a perception that a rigorous security-by-design approach will burden a project to an equal or greater extent.

The path forward

If done right, security-by-design is not a burden, and should not be considered optional. The way in which it is executed needs to be deterministic, and within the tolerances of the project management method. Security-by-design is then more than a set of steps, but rather a method with inputs, outputs and control mechanisms. It is a simple concept with far reaching consequences and results.

6
The key to security is implementing persuasive technologies

The default interaction between user and technology should enhance security

"Choose a password of at least 12 characters that include capital letters, special characters and that does not contain any regular names or words. Oh, and don't write it down." It's understandable that when making things secure, we'd like everyone to do as we tell them to do. Don't let your browser save your passwords, don't use third party tools, don't share documents etc. But then don't be surprised when people ignore your demands and go their own way, or try to circumvent your regulations. The only way to make people behave in a way that enhances corporate security is to make things easy for them, not harder.

It is one of the key signs of the time, and it goes against established ideas of how policies must be followed almost regardless the impact to the users workflow. Users interact more confidently with technology and value their autonomy in it. Luckily, with this more intimate interaction between user and technology also come opportunities. We can make the technology persuasive. We can build in subtle triggers and constructs that elicit the right

behavior in people. We can make it natural, logical or even fun to do the right thing.

"The psychology of security has a long way to go."
– The Cyber Security Manifesto

What is recent?

Users have the power to circumvent. Unless you've closed off all access to mobile networks, Internet and portable devices and data carriers, users will find a way to work the way they like. Instead of getting in the way of the employee getting his work done, security practices should be geared towards helping the employee in getting his work done.

"Cyber security is systems, processes of communication and especially people. If people are not convinced of this, the whole thing is shot. No security policy can succeed. Our role with CISO is also to be ambassador of good practices in my company."
– CISO at a manufacturing company

Why is this relevant?

You can say that the user is the weak spot of any system, but you can also see him as an enormous force for good: if we can create the right circumstances, the user can take something that has an inherent insecurity (communicating online with unknown third parties) and make it more secure (by using multiple channels to verify identity, being careful with attachments or by directing the collaboration to an outside platform etc.). Preventing unintentional leaks – think of the lost USB keys with customer data – is

the first obvious benefit, but it goes much further than that. The user can become part of your detection system to raise an alert when something happens that is out of the ordinary for example informing the support desk if a suspicious email slips through your email filters or when login behavior is suddenly changed. This way, users can help counter social engineering attacks and targeted phishing.

What new action should I take?

The most common approach today is to force restrictions on the user. Most companies use things like mandatory yearly training, restrictive guidelines and severe repercussions. They send out strongly worded emails that stress the importance of security and confidentiality. You may still use some of that, but most of the gain can be won in other areas:

> *"We expect a bit too much from employees. It is up to the company whether to protect and control their environment or not. We must find a balance and not fall into a totally unbearable situation for the user, with solutions thought up by experts who are not familiar with the company's business."*
>
> – CISO at a financial services company

- Rethink organizational processes with security in mind. For example, could you anonymize data in certain processes? Could you automate or better support processes that are now done through email?
- Give people small "rewards" and triggers for doing the right thing. This doesn't have to be gifts or monetary rewards, it can be any other kind of reward: for example give the user better insight into his productivity or skills, give the user social feedback, give the user the satisfaction of "completing" something

(e.g. a status bar that shows 100% complete when all actions have been taken etc.). There are many ways to make computer-human interaction more attractive by providing small triggers in the interface.

- Provide technical tools to make it easy: when you notice that people are using Dropbox, Gmail or some other tool that violates your security policies, don't simply ban these tools, but provide better ones that are under your control. Your own tools can be tied to your user database, making collaboration easier, they can tie into corporate search, making it easier to find stuff and they can be woven into other systems, making it easier for a user to jump back and forth between different tools (e.g. exception handling using corporate social networking). When asking people to follow complicated security procedures, think hard about technical solutions that would increase the ease of use: could a hardware token be more user-friendly than ever-changing password policies? Would a fingerprint reader satisfy our needs for security and make signing for approvals easier for your users? Could moving to a VoIP solution allow you to surface warnings when calls originate from suspicious numbers? Could single sign-on spur adoption of internal services and lead to reduced use of external tools?
- Make insecure things hard: the flipside is true too. If you've discovered insecure practices, you can change the settings to make these harder for the user. For example if users are storing too much sensitive data on their computers, you could decrease disk size. If people are emailing too many strategic documents, you could for instance decrease the size of attachments. This is a delicate path, since you don't want to push your users into even more insecure practices, so ideally you make the insecure things harder while at the same time making the secure things easier to do, helping the user make the change: for example offering a virtual desktop with unlimited space, many extra tools and more options to customize setting to your personal preferences.

"Bring encryption within reach of the average user."

– The Cyber Security Manifesto

Technology today can seduce, distract and engage us in a very social way. We've learned how to make apps and websites, the systems of engagement of today, which are tuned to make interaction easy and fun. If we ever want users to remember to do the right thing, we have to employ these same skills to make "being secure" easy for them, fun even. If ever you hear a user complain about some policy being too cumbersome, listen closely for it's an opportunity to improve it.

7
Fear as a tool is going blunt very rapidly

Organizations need to find a way to reframe the security conversation

Fear is a very strong motivator: it is essential to how our brain works. Other stimuli, even strong ones such as a good reward, have less power than fear. So when trying to get people to behave in ways that improve security (e.g. by using strong passwords, not sharing documents, not opening unknown links etc.), it is natural for security experts to use fear as the driving force: fear for the attacker, fear for data loss or fear for personal consequences. There are always great examples that serve to illustrate the horror when we fail to act as we're told.

There is a large problem with this approach, and it is that our main tool of fear grows blunt very rapidly. You can only tell a story once, and if the regular user doesn't see some real threat every now and then, they start forgetting or actively discounting your story. If you do a mandatory security training year after year, by the third year the impact of fear alone will be minimal, if the user has not seen any attacks happen that were the result of his actions or negligence. The human brain is wired for fear, but it is just as much wired for sensation, for change, and new stimuli. Any constant threat becomes the norm and loses its urgency.

From fear to value

Some companies have taken "being secure" as part of the core value that they bring to their customers. Here, security is not a necessary evil, it's a part of their value proposition: ingrained in the message to their customers, woven into the interaction with their customers and, consequently, a central part of everyday culture. Here "secure" is not only seen as a measure to prevent attacks, it's what helps make the company successful. What would it take for your company to become the most trustworthy one in the industry?

> *"I am impressed with the impact that I have at the level of management or business directions: I am listened to, my opinion is followed. It is a great responsibility."*
>
> – CISO at a bank

Of course, the value of security is real. First there is the obvious value of "having less risk," but it's more than that: in a society where people are interacting with many companies, "trust" has been called "the business-term for love." When markets are commoditizing fast, as they are, your reputation, branding, experience is what makes the difference and security is one of the most important values there.

> *"Cyber security is expensive to implement. Many companies take a pass on security because it is too expensive. I believe that we should look at this thinking economically: Is there no way to transfer a share of investment to an insurer?"*
>
> – Security consultant

Think once, act many

The trick to instilling security across the organization is to minimize thinking about security on a day-to-day basis. This may seem like a contradiction to creating a secure culture, but it's not. Create practices that make work life easy and efficient and that are inherently more secure. Take some time to rethink everyday activities and find alternatives that are better, easier to use AND more secure. For example: when people work on many files, why not work on them collaboratively online, without ever pulling them onto a portable device? When analysts work with large datasets, create the system in such a way that they can run all their formulas and programs on a superfast server instead of loading a lot of data on to their laptops. When customer service employees need to have access to customer data, show them only the data that is related to that specific customer based on the information the customer entered through the phone (so that they immediately have the right information but also could not browse or disclose information belonging to other customers easily). When your employees need access to many different systems, provide them with a single – two factor – authentication mechanism that works on all systems, so that they don't need to remember (or write down) multiple passwords. When you need to download files to your device temporarily, ensure that the data is automatically deleted after a certain amount of time. It guarantees that people work with the most current data, but also reduces the risk of theft. There are so many practices to think of to make life easier AND improve security overall.

To pivot from fear to value is not an easy feat, and most likely you will deploy a mix of both: show the value but use fear every now and then to get the attention. In the end it goes back to designing security into the things we do, into our technology but also into our everyday practices. This starts at the top and permeates the entire organization, as any organizational culture should.

8
Be your own worst enemy

The only way to find your weak spots is to really want to find them

Big differences between an attacker and a defender are often the determination and communication. When the attack becomes a group project, the contest aspect of the "game" doesn't work in your favor. The only way to balance this game would be to instill the same determination, communication and creativity inside the organization, with or without third party assistance such as a professional white-hat hacking team.

> *"Crime adapts and follows; there are new technologies, but crime is changing at the same time. Thieves are always a step ahead. They have more imagination than those protecting information, we face things we had not imagined."*
>
> – Security consultant

What is recent?

With the increase in the number of attackers who are in it for financial gain or with political motivation, the determination of some of the attackers has risen considerably. On the other side,

the increase in penalties, the increased enforcement of laws and high-profile convictions have scared away a lot of the low-harm script-kiddies leaving "only" the more professional attackers in the game. The oft-used term Advanced Persistent Threat (APT) alludes to their frantic determination: the attackers are willing to spend a prolonged period of time to breach your defenses and then keep using their access for an extended period of time, with prolonged access to your data. Where traditionally attackers would find an exploit and then try it out on many different organizations, in the current environment more often an organization (or person) is singled out and then attacked in a multitude of ways.

Why is this relevant?

Both ignorance and determination threaten our security: if your own people are completely ignorant, there will be no security or if the attacker has great determination, the common expectation in today's security world is that ultimately he will get through. By addressing both internal ignorance and motivation, and heightening your defenses to only let through the very most determined, you can achieve a workable security situation. The goal is as always: to remain one step ahead.

What new action should I take?

In the common approach of today, the emphasis is on applying patches, designing a secure infrastructure and educating users. Some thought is given to considering "the most viable attack," but it's not yet a cornerstone of corporate security. Develop a hacker mindset and find your weak spots before others do:

- Regularly use (or create your own) white-hat penetration test team, who are challenged to break in and get to systems or data they shouldn't have access to. You could create a permanent "red team" that could take all necessary time and means to get on par with modern hackers. You could even rotate some people between the "defense" and "attack" teams every couple of months to make them see both sides of the issue.
- Make it a game: There are many ways to turn security into a game for the entire organization. There have been examples of people losing game-points for leaving their laptop unlocked and winning points for spotting someone without displaying an access badge or finding files that should not be openly available. Gamification of security brings a positive spin to the security discussion and increases awareness *and* compliance to security protocols.
- Make sure you have responsible disclosure procedures: there should be an easy way for outsiders to contact you, if they happen to discover security flaws at your company. Responsible disclosure is delicate (you don't want to encourage people, yet do want to learn of issues), but has to be available and it has to be very responsive. Whenever someone reports an issue, they should see quick follow up and possibly a reward of some sort.
- Understand the (potential) attackers: just like you want to understand the organizations most valuable customers, organizations would like to understand the most damaging adversaries too. Where are they from, what is their motivation, what is their market etc. When the focus is on technology only, it's hard to anticipate. Getting a better picture of possible attackers requires planning in scenarios: who might attack, for what goal, what would be the intended and unintended consequences and what can organizations do to counter them, either in taking away their motivation, their market or by disrupting their attack.

"For example if the company signs a controversial contract, they must notify the IT department that there is a sensitive contract that might be exposing the organization to attacks. And yet, this idea does not come to them often!"

– Cyber activist

The puzzle dimension of hacking is great fun: trying to find a way to execute some code, to pry loose a small part that leads to a gaping hole. The same drive that motivates hackers, if present in your security team, can be a great asset for the company. Making it fun also prevents tunnel vision, and it enhances the creativity that is needed to finds the real weaknesses in defenses. Understand attackers, and try to be like them, a little bit.

9
You will be hacked, but it's OK

As long as you know it and can recover

What happens when the most dedicated people put all their attention on you or your company? That thought alone is enough to scare anyone: you cannot trust any email, attachment, document, phone-call, visitor, WIFI network etc. The tales from white-hat hackers who prove they can do almost anything from hacking turn-styles to social engineering their way into the accounts of top-management give a glimpse of all that is possible. We can assume this is also true for the criminals and some other adversaries. So what can you do? Should you surrender and simply sit back and let it happen? Of course not, knowing that true dedication will compromise your defenses prepares you to work on minimizing the effect and increasing the chances of detection.

"The question is not can I be hacked, but I can be resilient?"

– CISO at a financial services company

What is recent?

There have always been very targeted attacks, especially in the defense industry and in the financial world. These days, the number of dedicated players has increased, with professional crimi-

nal groups spending most of their time online. While Advanced Persistent Threat is often used to indicate attacks by state or "business" players, the "private" hacker community is sometimes acting in a very similar way: coordinated hacker communities target individuals or companies for hacktivism reasons: political or social issues that enrage a certain group of society, who then resort to hacking to make their point or influence the public discussion.

> *"At the banking level, we have an image, we represent capitalism, we represent the bad guys. Suddenly, we live with threats on a daily basis. We monitor all online activists, we prepare ourselves to be able to fight."*
>
> – CISO at a bank

Why is this relevant?

The Advanced Persistent Threat is, perhaps together with the inside threat, one of the most serious threats that an organization faces, as bullet-proof defense is virtually impossible yet the damage can be enormous. Persistent attackers are not afraid to influence your organization's staff, or even purposely get hired, to get access, making detection even harder.

What new actions should I take?

In the traditional view of security, the focus was mainly on defending the perimeter, on maintaining security and preventing for example the exfiltration of data. But then, once defenses were breached, or data was exfiltrated, the damage was done and all organizations were left with was closing the holes and living with

the damage. So what can organizations do differently knowing about Advanced Persistent Threats?

"The most important thing for us is recovery."
– CISO at a bank

- First of all set up counter measures across the whole process of the attacker: from trying to take away the driving motivation, right until the actual attack and possibly publication after the attack. This is setting up the so-called "Kill-chain."[1] By understanding the process attackers follow, you can try to detect, deny, disrupt, degrade, deflect or deceive attackers every step of the way.
- Even more diligently monitor your network and systems: as long as you are unaware of what's happening on your network, you have very little chance to detect any sophisticated attack. Many organizations that know they have been breached were alerted months (or years) after the initial intrusion, most often by outside bodies such as the police of security researchers.
- Proactively minimize the effect that breaches could have: for example by encrypting data at rest, by adding fake data to real data – so that stealing a million credit-card numbers would in reality only contain a thousand real credit cards and close to a million fake numbers.
- Reactively minimize the effect that breaches have: immediate communication and remediation, customer focused solutions or compensation for customers who were affected.

So, even while an organization will get hacked, look at it as losing the battle but still winning the war. Make sure that every step of the battle was hard and long for the attacker: wading through every layer to get to just small pieces of data. Even threats that do succeed to break through should only get away with a few tidbits

1 More on the kill-chain here: www.appliednsm.com/making-mandiant-apt1-report-actionable

of data, and not be able to gain complete access with one break-in. Meanwhile, you're watching, ready to catch them in the act.

10
The data scientist will be your next security superhero

Pattern recognition is not a common IT security skill

Can you predict what actions are bad, and which are good? Can you segment users based on their behavior into risky and regular? Can you detect when a disgruntled system administrator is installing malicious software right before he leaves the company? Such are the questions we're trying to answer by applying advanced security analytics to big data. This advanced analytics involves models for representing threats, attacks or even heuristics of observations. These analyses need data for training and teasing out patterns. Sometimes these analyses are meant solely to provide visualizations so that that human knowledge can be applied to derive insights. By connecting data from system log files, historic data about IP addresses, honey pots, system behavior, user patterns etc., we can build a much more complete picture of what comprises normal behavior for a user or scenario. The trick is to combine many different sources and look for patterns across these different systems that indicate undesired behavior. Advanced analytics on big data can be used to detect external breaches – for example by detecting patterns in behavior of attackers when they do reconnaissance, but also to detect internal risks – for example by automatically alerting when someone is accessing unusual data at an unusual time. There are already many benefits that can be achieved without big data, sim-

ply by looking for what happens across the silos but the promises of big data are even more ambitious and pro-active. Alas, it may be hard for a regular security team to achieve any results from the big data part, unless they hire a true data scientist who can help find patterns or help make sense out of the patterns found.

> *"We may have effective detection tools to reduce the impact of the attacks. But the real revolution will be with big data: We will be able to more finely analyze what is normal and what is not normal."*
>
> – CISO at an electronics company

What is recent?

The IT industry has recently discovered the value of big data and the information that can be hidden in large and disparate data sources. This renewed focus on data has also bled over into the security community, applying similar technologies to the data sources available to detect and prevent attacks. New technology and analytics make applying an advanced analytic big data approach possible now.

Why is this relevant?

The data side of the story is about breaking down data silos in support of advanced analytics. We already can collect large volumes or even high-speed security data but now we want data from other places as well. In the analysis it is not so much about finding the good and the bad, which is almost intractable, but rather knowing what is "normal" so as to allow for analyzing the exceptions. Traceability and linking become crucial whether you are observing data flows, conversations or entities. This prom-

ise is encouraging many organizations to embark on this journey. Any mechanism that gives deeper insight into the unusual, abnormal and potentially malicious in an organization would be a great addition to the arsenal of tools available.

What new actions should I take?

Without using advanced analytics on big data we would have almost too much data: log files that are larger than anyone can ever analyze, let alone cross-correlate with other log files, HR data and whatever other sources we might have. We need technology to help us find relevant data, or the data is useless. Some even claim that the current way of using data is actually hindering security because too much time is spent while results are thin. So what to do?

- First, get a realistic understanding of what advanced security analytics on big data can and cannot bring to your detection mechanisms. While the promise is attractive, the reality is a bit more complicated, since there is no guarantee that patterns will actually be found, or that these patterns will hold up in the future. What if during the time of annual reports, suddenly all alerts start sounding because all kinds of people start accessing data that they "normally" didn't use? Can you use your data to prevent an attack, or is quicker detection when there is an attack the best you can get?
- Hire or reassign people who do have the data skills necessary: the data scientists or business intelligence buffs. They need to know about patterns, statistics, correlation and how to use the tools and insights operationally.
- Start collecting and correlating data across different systems, levels and channels. For example, when the HR system flags someone as "at risk of being fired or leaving," that should also factor in how the behavior of that user is analyzed. Logs from

across cloud, on premise, mobile and internal need to be transparent, etc.

"Securing the cloud means redefining it as an end-to-end secure system."

– The Cyber Security Manifesto

Better insight leads to better decisions. This is true for security operations as much as for any other business function. If currently you are operating completely in the dark, still working with large log-files from separate systems, it's like trying to run a business without something as basic as accurate sales or inventory numbers. Beyond that basic level lie the innovations that promise to automate much of what today is still manual labor. big data may well be an entry way into smarter systems that practically secure themselves.

11
Hackers learn quicker than the organizations they are attacking

It's time to stop making the same mistake over and over

When the phone systems of the past were hacked, it was by applying "control" codes in the "content" of the call: sending special tones during the call could give you access to unlimited free calls or calling at someone else's expense. Yet when we introduced databases the same thing happened: we mixed content and control codes in the same "channel," thereby making it possible to inject control codes into the content: SQL Injection. It seems that with every new technology, we are re-learning the same lessons on how to make things secure. Hackers know this and whenever a new device or application comes available, they diligently try out all things that worked in the past on other devices or applications: using overflows, disrupting control, injecting, overwhelming, etc. Hacker communities are famous for spreading their knowledge quickly, even training young "apprentices" to become better. The only way to play the defense in the same way is to do the same: diligently apply lessons from the past and work collaboratively to learn fast.

"Cybercrime has greatly evolved; we went from poorly organized operations to organized crime. Criminals exchange a lot of information, and they are really very advanced. On our end, we must make that leap, too, and also share our experiences and best practices. Everything related to the threat, how the incident was detected, analyses that were made, and how it was managed; the community should be able to use this, and everyone can benefit."

– CISO at ministry of finance

What is recent?

With the introduction of new devices, new API's, Cloud and collaborative business processes, the number of places where attacks can be orchestrated has multiplied. We can expect that soon the lessons from "hacking systems" will also be applied to the human-computer interaction: providing more vectors to influence people to take actions that compromise your integrity.

Why is this relevant?

With every year, we gather more experience, but this is only relevant if we actually apply the knowledge gained. If we forget lessons from the past, our most recent insights are useless. If we run the latest version of a dynamic, data oriented perimeter security system, but we forget to apply a password policy for our users or for example use live data in test environments, the advanced security system has little value.

What new actions should I take?

In the race to beat the attackers we are always on the lookout for the latest and newest threat and counter measures. We are trying to keep up with a very dynamic field of technology innovation so naturally our focus is forward-looking. Yet with the passing of time, our "stack" of historical "best practices" has grown significantly, it's time to work together across companies to build a solid body of knowledge of our industry:

> *"The only way to effectively fight against cybercrime is to form inter-company teams. Individually, each in their own corner, it will not happen."*
>
> – CISO at a bank

- Of course, know and apply the industry standard frameworks that cover information security. If you are still inventing everything yourself, you're not re-using information created by others.
- Learn about the conceptual, abstract side of attacks: what kind of patterns are there, how are they applied in different layers and technologies, and how can we counter them. Then, whenever a new technology will be introduced (for example the "Internet of Things"), you can quickly gauge what patterns could be applied and how to design your system securely to minimize risk.
- Become a leader in the community when it comes to security: take a pro-active stance to not just participate but push forward security practices in your industry, supply chain, country etc. The best way to get your own security practices to be best in class is to strive to be the leader in the field; setting the standards instead of just implementing them.

Security professionals are traditionally bad at sharing experiences, for fear of giving adversaries insights that could be used

to attack. Yet the upside of sharing and a strong international security community would far outweigh the risk to the individual company. Imagine the entire security world collaborating to create a secure and reliable Internet, sharing detection methods, pointing out bad guys and conceiving solutions together. It's the only way for the good guys to gain a sustainable advantage against the bad guys.

12
Encryption is just another arms race

What is good enough today will not suffice tomorrow

Has RSA already been broken? Can we still use PKI? Do our electronic "tokens" still really protect our network? We tend to assume that certain things are "secure" and can be "trusted," but time and again, our trusted friends in the struggle to maintain security get broken. The advance of technology innovation is brutal and doesn't stop for security considerations. More computing power, parallel computing and new computing paradigms are threatening encryption mechanisms that we use every day. There are strong rumors that some organizations have already found ways to decrypt any encryption commonly used online, including the ones used for https. Encryption plays a vital role in everything we do, from asserting identities to securing confidentiality and transaction integrity, so any threat to this key component represents a cross-system vulnerability of the greatest magnitude.

"We do expect not technological revolutions, in this area, it is quite rare."

– CISO at an electronics company

What is recent?

Moore's law was already scary, promising to make swift what used to be slow, but the advent of Cloud puts this in overdrive. Anyone can spin up thousands of computers in an instant, making brute-force attacks easier than ever. And what will quantum computing bring? There is a lot of buzz and research in this area and if it really delivers on the promise, it will instantaneously reduce the value of encryption mechanisms that we've been using up to now.

Why is this relevant?

When an encryption mechanism gets broken, it needs to be replaced with a new one, that much is clear. But is it that easy? And have these new mechanisms been proven? What about your old data that was encrypted? If any was stolen in the past, it could mean that it's now out in the open.

What new actions should I take?

You may be basing your policies on the assumption of "encrypted = safe," but this needs some nuance:

- Assess pro-actively what data files could have been stolen in the past (perhaps even without your knowledge) that could, with current or near-future technology, be easily decrypted. Which organizational risk would this carry? Especially for data has a long life span, this risk may be large: personal data, Intellectual Property, DNA profiles, fingerprints, controversial internal communications etc.
- Create a high level plan of action for when your encryption mechanisms will need updating: what systems need to be

changed, what data needs to be re-encrypted, what tools and applications would suffer because of low backward compatibility etc.

- For information that needs true long term protection, yet can still possibly be stolen or leaked, use the strongest encryption mechanisms available today, to delay the inevitable as long as possible.

"The defense roadmap must be ahead of the attack roadmap."

– CSO of a research institute

The reality of security is that it really is a game, or an arms race. Hard math will become harder, the tools of today will be enhanced and complemented with new and more powerful tools and science is challenged to come up with the next, harder to break, method of encryption. And the more valuable and long-lived your data-assets are, the more essential it is to be at the cutting edge of innovation.

13
The mobile revolution has blown the lid of Pandora's box

Your life will be hacked and only changing your habits can restore security

There are many developments that have shaken the world, but few have gone as fast and have had such a far-reaching effect as the adoption of smartphones and other mobile devices. This explosion of devices and associated usage has obvious security implications: not only are these devices relatively new and thus largely untested when comes to security, they are small and light, and we carry them in our pockets and briefcases, which increases the risk of loss or theft.

The risk of these devices is composed of several elements:

1. **Mobile device variation is increasing** – There are now smartphones (with many different operating systems), tablets, ultraportables, smart watches sports trackers and soon there will be smart cars, smart glasses and basically "smart anything." The Internet of Things is upon us, and the security implications are far from clear. The one thing we can assume: with increased variation it becomes practically impossible to come up with one security technology that covers all. The number of different devices looking to connect to our corporate networks

and systems is increasing every day, possibly presenting new vectors of attack.

2. **Limited security** – These mobile devices have limited capabilities for effective built-in security and even if they do, many users don't actively secure their devices. Some users even "jail-break" their devices, taking away some of the security measures that are part of the original setup. Jail-breaking in itself is an interesting example of control/security measures backfiring: users who feel too constrained by the restrictions imposed by device makers or carriers then break this constraint and in the process may abandon more security than they are aware of. Meanwhile, the power of these devices has become phenomenal, so they can be used as an entry way into other systems, e.g. as botnets to carry out attacks or any other application an attacker sees fit. All you need is a compromised app, a link, a document or even a text message.
3. **Loss and theft** – Meanwhile, cell-phone theft accounts for 40 to 50 percent of all crime in cities like New York, Washington DC or San Francisco.[1] In the USA, nearly one in three people reported they had experienced a lost or stolen phone.[2] Smartphones today carries more value and potential for disruption than our wallet. Through a gradual adding of functions and loading new apps, we've now connected everything to this single device. It is exactly this combination of functions that makes the device so valuable to users. And while losing your wallet was already a hassle, losing your smartphone could mean an instant threat to all your online and offline assets: social media, finances, communication, pictures, contacts, ideas, notes, … Even your company's secrets are instantly at risk.

1 http://www.marketplace.org/topics/business/cell-phone-theft-rise-industry-isnt-helping-much-infographic

2 http://pewinternet.org/Reports/2012/Mobile-Privacy/Main-Findings/Section-3.aspx

"What scares me? Connected objects, on which the company will become dependent. What will happen if extremist movements attack these objects?"

– CISO at a global hospitality company

Why is this relevant?

Adding all this up, the likelihood of any individual experiencing a theft, hack or attack is becoming very large, with potentially serious personal and business risks.

What new actions should I take?

Changing behavior starts with realizing the value of your information

In everyday life, you may not consider the value or potential for disruption that a lost or compromised device may represent. We balk at long complicated pass-codes, we dislike automatic screen-lock or the threat of a remote-wipe feature, because usability is what attracts us to these devices, and most measures make the device ever so slightly less easy to use. Still, when you realize the mess you could be in when someone purposely takes your phone, looks at all the photos, reads all the messages and uses all the apps to access your mail-accounts, social media, business VPN etc., it becomes much more acceptable to use stronger security measures.

When there is at least a basic desire to remain secure, a lot is possible: you can store as much as possible on servers or in the cloud, instead of on the device (and then don't store the passwords on your device), use strong login codes, activate the automated screen lock, enable the remote-administrator capabilities so you

can wipe or lock the phone when it gets lost and of course, most obvious: treat the phone like any other computer when opening links or downloading apps, games, screensavers etc.

> *"Security should be as quality was 30 years ago. Little by little it has become indispensable for all employees. The day where we will have managed to make people understand that security is part of their everyday work, we will have won!"*
>
> – CISO at an electronics company

Meanwhile, technology is catching up and increasingly available to help the user be secure: tools are emerging with which your organization can systematically scan your phone for threats, you can use anti-virus measures on the device, there are dual systems where business and private use are completely separated, etc. Still, here too counts: if you don't have the desire to remain secure, you're many times more likely to get hacked.

Mobile devices are here to stay, and they will become smaller and even more ubiquitous. Just like with cars, planes and other inventions, a little while after massive adoption, the public will start to really understand the risks and required behavior to remain safe while using new technology. Seatbelts in cars and safety briefings in airplanes are common today. For mobile, it's time we get started.

14
All eyes on security

Using the confluence of technological change to drive security outcomes

There is a greater emphasis on, and understanding of, security threats and challenges than at any point previously. Both the general public and executive management of public and private organizations are focused on the issue and are in search of answers.

For years, security professionals have struggled to get budget, to be included in the initial design of products and services and to help business leaders without deep, technical expertise understand the impact and necessity of security projects and programs. However, over the last few years many of the warnings about the potential about what "could" happen has moved from theoretical threats to real breaches and incidents. The costs are rising. The damage to many brands around the world has already been done. There will always be further opportunity to raise awareness about security challenges, but today the world is intensely focused on what is being done to beat back the seemingly endless tide of disclosures, identity theft, fraud, espionage and cyber attack.

While security professionals may have preferred to reach this level of focus and understanding without the incidents that have been splashed across newspaper headlines for the few several years, it is difficult to deny that the time is now. This is the opportunity to affect change.

The world is entering an entirely new generation of IT focused on cloud and mobile technologies, and the exploding amounts of data moving between these systems. As organizations embark on preparing their infrastructure and workforce to be both cloud and mobile first, there is a truly significant opportunity for security teams to embrace change and play a key leadership role in these transformations.

Whether referring to the grid, web applications or even the Internet itself, it is a common chorus to hear, "these were designed originally without security as a core consideration." Decades have been spent bolting security on after the fact, but the reality about initial design remains inescapable.

The challenge and opportunity of today is to avoid repeating the same mistakes of the past. There are critical, transformative technologies being designed and built right now that will have a lasting impact on the world and they are reaching maturity at a moment where the focus on security has never been more significant.

This is a time when business leaders must demand that their security teams help lead enterprise transformation and when security teams must rise to the opportunity they have sought for the last thirty years.

Today, it is all eyes on security.

About the authors

Erik van Ommeren
Director of Innovation at VINT Research, Sogeti
www.linkedin.com/in/erikvanommeren

Martin Borrett
Director of the IBM Institute for Advanced Security Europe
www.linkedin.com/pub/martin-borrett/0/633/660

Marinus Kuivenhoven
Senior Security Specialist, Sogeti Netherlands
www.linkedin.com/in/marinuskuivenhoven

Index

About Sogeti

Sogeti is a leading provider of professional technology services, specializing in Cyber Security, Application Management, Infrastructure Management, High-Tech Engineering and Testing. Working closely with its clients, Sogeti enables them to leverage technological innovation and achieve maximum results. In the field of Security, Sogeti provides services to assess, improve and monitor security, both in technology as well as in policies and organization.

Sogeti is an IBM premier business partner who brings together more than 20,000 professionals in 15 countries. They are present in over 100 locations in Europe, the USA and India. For more information please visit www.sogeti.com.

About IBM Security

IBM's security portfolio provides the security intelligence to help organizations holistically protect their people, data, applications and infrastructure. IBM offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. This comprises 10 security operations centers, nine IBM Research centers, 11 software security development labs and an Institute for Advanced Security with chapters in the United States, Europe and Asia Pacific. IBM monitors 15 billion security events per day in more than 130 countries and holds more than 3,000 security patents.

VINT | Vision • Inspiration • Navigation • Trends

HTTP://VINT.SOGETI.COM

SOGETI
IBM SECURITY

ISBN 978-90-75414-77-6