BLU SPHINX

Principles of Cyber Security

Thomas Dillig, PhD Aurelie M.H. Beaumel General (Ret) Jean-Paul Palomeros

Summary

Cyber security has become a key priority across the world, relevant to all actors of human societies: international organizations, national governments, businesses, and individual citizens. However, cyber security remains a generally poorly understood notion, with unclear boundaries and goals. Our objective in this white paper is to define fundamental principles of cyber security and lay out a new foundation for a comprehensive and long-term strategy aimed to increase the security of organizations and individuals in the cyber space. We believe that cyber security must be on the agenda of every public or private decision maker. Although cyber security shares principles with other types of security, the cyber space presents challenges distinct from other areas. In order to protect critical systems and data of any organization and to prepare for emergency crises that may arise from increasingly frequent cyberattacks, it is a essential to be proactive and to develop appropriate cyber security policies. We believe that cyber security relies on three equally important, inter-connected areas: Technology, Strategy, and Human Behaviors. As top priority, it will be crucial to develop central repositories of knowledge and technologies to guide organizations in implementing the best cyber security strategies and effectively respond to attacks. It will also be crucial to explore one's strategy and choices carefully before a real attack happens, in order to validate trade-offs under attacks. Simulated environments offer a unique opportunity for interactive learning and strategy testing, without incurring the potentially catastrophic cost of real attacks, to determine the appropriate course of action.

Cyber security has become a key priority across the world, relevant to all actors of human societies: international organizations, national governments, businesses, and individual citizens. Cyberattacks are becoming both more frequent and sophisticated, resulting in increased reach and damage.

Introduction

Cyber security has become a key priority across the world, relevant to all actors of human societies: international organizations, national governments, businesses, and individual citizens. Cyberattacks are becoming both more frequent and sophisticated, resulting in increased reach and damage. These damages include massive losses of personal data [1, 2], loss of strategic data [3, 4], money theft [5], disruption of critical infrastructure [6], disruption of a democratic process [7], overloading of Internet servers [8], and many more. All of these attacks have resulted in significant material and financial losses, customer loss, very high legal penalties, reputation damage, and could even threaten human lives in the future (medical devices, health services, emergency systems, etc).

However, cyber security remains generally a vague notion with unclear boundaries and goals, poorly understood by decision makers and the general public. Even among military and civilian experts (technological researchers, policymakers, law enforcement, specialized organizations, etc), there is currently no consensus and common understanding on which principles, techniques, and policies should be used and promoted.

Since cyber security affects all areas of society and organizations, it must be part of an overall risk management strategy that includes the assessment of risks and trade-offs across divisions and possible ways to mitigate them. We believe that cyber security must be on the agenda of CEOs and other top decision makers. It cannot be confined to technical units who may be limited in their influence over entire organizations. Developing effective and comprehensive cyber security strategies requires a big-picture perspective.

Our objective in this white paper is to define the fundamental principles of cyber security and lay out a new foundation for a comprehensive and long-term strategy aimed to increase the security of organizations and individuals in the cyber space.

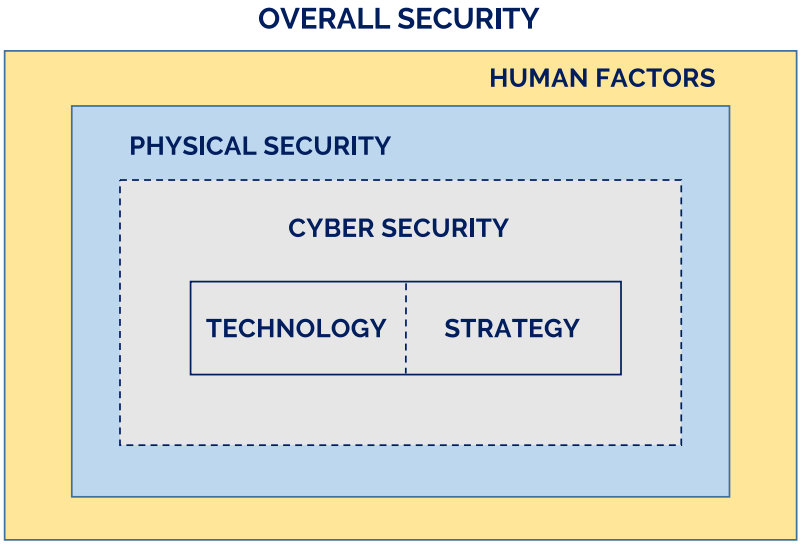


Fig. 1: *Any security system is only as strong as its weakest link.*

Security in the Cyber Space

The concept of cyber space is commonly used to refer to interactions between publicly networked computers on the Internet. Over time, a virtual world connecting all areas of societies, organizations, and people's lives has developed in an organic and resilient eco-system. Cyber security is the security of networked information systems and data.

However, cyber security is only meaningful when viewed in the general context of global security, which is a requirement for ensuring a peaceful and prosperous development of human activity. Cyber security should therefore be considered as a key piece of an overall risk-management architecture that includes notably physical security and human factors. This global security approach should not be contemplated as the mere result of adding security measures which would excessively constrain the digital transformation and dramatically reduce its beneficial outcomes. Instead, developing appropriate cybersecurity policies needs a new attitude, shifting minds and processes from risk aversion to risk mitigation, and ultimately to risk management. In the cyber space, man-

Cyber security is the security of networked information systems and data. Although cyber security shares principles with other types of security, the cyber space presents challenges different from other spaces.

aging risks implies a permanent process of threat assessment.

Enhancing cyber security by making software systems and data more secure does not increase overall security if other security components (physical security or human factors) remain relatively weak. For instance, if an organization equips itself with the best cyber security technology to manage a database with confidential information, but grants access to the database to a wide range of individuals without sufficiently vetting their reliability, the confidential data that the organization is trying to protect will remain vulnerable, regardless of the database technology used.[1] Any security system is only as strong as its weakest link. Even the best cyber security strategies require a comprehensive security analysis of the environment in which systems operate and data is stored (or sent). Cyber security will only keep data and systems as secure as the surrounding security allows.

Properties of the Cyber Space

Although cyber security shares principles with other types of security, the cyber space presents challenges different from other spaces. Due to the idiosyncrasies of the cyber space, some concepts applicable to physical security need to be revised in the context of cyber security. Traditional security analogies are sometimes misleading. We will focus on the notions of Discovery, Attribution, Prevention, and Deterrence to illustrate this point.

Discovery

The first step in dealing with an attack is to discover that it has happened. In the physical world, this is relatively easy because many attacks leave an observable physical impact (disappearance, damage, etc). On the other hand, in the cyber space, attacks do not necessarily leave any observable impact. Cyber theft does not necessarily require the removal of the stolen information from the system. Infiltrating the system and making a copy of the data, unnoticed, accomplishes the same objective and damage. Therefore, securing a cyber system entails building a system not only capable of withstanding cyberattacks, but also able to detect if it has been breached. In contrast to physical attacks, discovering that a cyberattack has been perpetrated is a challenge in itself.

Attribution

Also in contrast to the physical world, it is significantly more challenging to identify the guilty parties once a cyberattack has been detected. By its very nature, the Internet is designed to make it difficult to connect an action in the cyber space with someone in the physical world. It is a very hard and labor-intensive guessing game to find out where attacks come from and to prosecute cyber criminals. This difficulty arises because there are multiple layers separating a cyberattack from its authors, starting from where the attack took place, to the physical device used to conduct the attack (which may be on the other side of the world), to the specific person who used the device. Additionally, using non-technical approaches to try to solve this problem, such as passing legislation, cannot be effective. Due to the inherent anonymity of the Internet (or at least its ambiguous identification), the problem of attribution remains a challenge unless one is willing to break down the Internet. While it is possible for nation-states and large organizations to pinpoint the source of an attack accurately with additional intelligence, smaller businesses and all the more so individuals do not have access to such resources and remain defenseless.

Prevention

Given that cyberattacks are more difficult to identify and attribute, and can have disastrous consequences for organizations, businesses, and individuals, preventing them becomes critical. Cyberprevention currently relies on approaches that are well-known but need to permanently adapt to new threats (firewall, antivirus, cryptography, etc). However, this technical approach is not enough on its own, and must be part of a comprehensive view of the activities of an organization (or person) and their vulnerabilities. Such a global approach should also take into account the interactions and dependencies with other organizations, suppliers, and the potential cascade effects (shared databases, physical security, In-

[1] The case of Edward Snowden is a compelling example with gigantic consequences.

Communication and training are two powerful levers of cyber-prevention. There are many who do not have basic knowledge of the principles and systems that increasingly govern our daily lives and activities.

ternet providers, providers of cyber security systems, etc). Above all, effective prevention relies on all actors of an organization, not only cyber security experts.

Communication and training are two powerful levers of cyber-prevention. It is important to remember that there are generations of people who have not been raised nor educated in a digital society. There are many who do not have basic knowledge of the principles and systems that increasingly govern our daily lives and activities. Even for younger generations who master the use of digital tools at a precocious age, there is to date no widespread education program to teach children and teenagers the fundamentals and risks of digital activities. There is no driving license or academic certificate required to navigate the cyber space.

However, prevention should not be viewed only through a limiting or repressive lens. It also provides a great catalyst for imagination, creativity, and transformation. As example, in the fields of aeronautics and aerospace, the need for reliability and security stimulated innovation and drove a deep change in cultures, methods, and organizations, leading to well-known improvements in terms of reliability and growth. An ambitious agenda for prevention of cyber attacks needs to rely on human assets and enable everybody to become a stakeholder and strong link in the cyber security chain.

Deterrence

In many defense-related contexts, deterrence is a commonly used principle (mutual retaliation, mutually assured destruction, etc) that discourages attackers by communicating that the costs of attacking will be very high, or too high, for them to bear. As criminals are more difficult to detect and catch in the cyber space, it is unclear how threats and deterrence can effectively work for cyber security, except for large-scale hacking operations sponsored by nation-states.Any deterrence approach relies on the credibility and resilience of the means of deterrence. It also assumes that the potential aggressor can be identified without doubts. These requirements are hard to meet in the cyber space. First, capabilities for cyber-deterrence need to be developed by nation-states to guarantee their legitimacy and legality. However, there are major actors of the cyber space other than nation-states who master and even define the rules of the game, security, and tools. Which role are they ready to play in a logic of deterrence? One could add deterrence against cyberattacks to a global strategy of deterrence. The 28 members of the North Atlantic Alliance have decided that some cyberattacks, particularly powerful and/or destabilizing agains one of the Allies, could fall under the collective defense clause from article 5 of the Washington Treaty. This is a major step towards the recognition of cyber threats, but also presents limitations. As mentioned above, attribution is a challenge in the cyber space, but is also a prerequisite to trigger an appropriate response. It is publicly known that some nation-states are hiding under the identity of hackers groups responsible for massive targeted attacks ([3, 7, 6]). In the cyber space as in other spaces, deterrence requires to be armed, which means developing sophisticated intelligence and credible offensive capabilities. However, for obvious reasons, nation-states developing such capabilities do not advertise them and make at most a statement of principle.

Additionally, the use of deterrence may not be possible against criminals who (1) possess nothing of value to be attacked on, (2) are willing to cause harm for no direct gain (financial, territorial, strategic), and (3) are willing to "die for their cause". These include non-state actors such as terrorist organizations or regimes with an "end-of-times" view. This issue of asymmetric threat affects all areas of defense, including cyber defense. There is a need for cyber security and defense strategies that can work with different types of threats. Deterrence is undoubtedly on of these strategies, at least for nation-states with ample means. But if deterrence methods are difficult to apply for all non-state actors and for nation-states as well, an essential approach to counter cyber threats is by designing secure cyber systems.

Three Pillars of Cyber Security

In order to take any cyber security policy to the next level, it

We believe that cyber security relies on three equally important, inter-connected areas: Technology, Strategy, and Human Behaviors.

is necessary to establish strong and concrete foundations. We believe that cyber security relies on three equally important, inter-connected areas: Technology, Strategy, and Human Behaviors.

Strategy directs decision making and organizational processes, as well as means to achieve a specific objective. It therefore entails making the necessary trade-offs for securing and organizing data and systems.

Technology encompasses the science, techniques, and tools designed to disseminate, use, store, and protect data and software systems. It depends to a great extent on human behaviors for its efficient use. What sets apart digital technology is the speed at which it evolves. The constant increase in computing power with increasingly smaller devices and the important data flows are all factors of the digital transformation that applies to virtually all aspects of human activities. The ability to explore vast amounts of data to extract insights (Big Data Analytics) will lead to predictive analyses that will influence the behavior of decision makers as well as populations. The Internet of Things is paving the way for new applications that will transform our daily lives. Artificial intelligence and machine learning will accelerate the automation of some functions, such as advance the field of robotics. This digital revolution presents opportunities for unprecedented progress, but also presents major risks, especially to secure the data fueling all these advances. The success of the digital transformation will depend on the ability of humans (developers, leaders, decision makers, experts, operational teams, etc) to define objectives, limits, rules, and ensure security.

Behaviors include the human knowledge and behaviors in the cyber space necessary to reduce the effectiveness of cyberattacks, including the appropriate use of cyber security technology. Humans are ultimately responsible for to orient, prioritize, develop, and implement any cyber security policy. In this respect, it will be necessary to develop new methods to manage complexity, to break down the existing silos of society and foster horizontal cooperation between experts of different backgrounds. Efforts to raise awareness, educate, and train actors of society at all levels should be a top priority to develop a long-lasting and efficient cyber security. In cyber space, the security of all depends on each one of us.

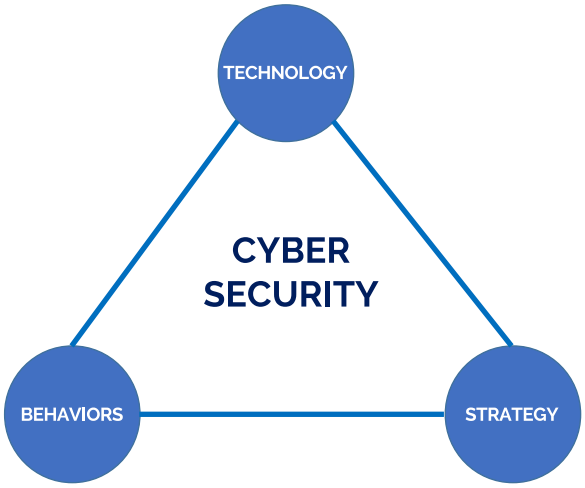


Fig. 2: *The three pillars of Cyber Security.*

Technology: Building more Secure Cyber Systems

Cyber security deals with the security of software systems, whose fundamental basis is discrete mathematics and logic. This is the key difference between software engineering in the cyber space and the physical world where the fundamental basis of classical engineering is continuous mathematics. The discrete nature of software makes the standard engineering approach of "overbuilding" impossible. To illustrate the point with civil engineering, if one needs a structural steel beam that can hold 10 tons, one would design and manufacture a beam sturdy enough to hold 12 tons to ensure that it will be able to hold 10 tons, irrespective of small anomalies that may occur. Such an approach is impossible for software security because the security of any soft-

We believe that attempting to reactively protect fundamentally insecure and ill-designed systems is an expensive and ultimately futile exercise. Reactive security can only be truly effective on top of a properly executed cyber security strategy that puts secure and layered systems in place.

ware is a binary property. There is no such concept as "a little bit hacked". A software system is either secure or hacked.

Security measures can also be either reactive (e.g. putting out a fire) or proactive (e.g. using fire-proof materials). Since it is challenging to design proactive security approaches, there is currently substantial focus on reacting to and managing breaches as they happen. While this strategy is capable of limiting damage in the case of attacks, the war against cyber attackers will be won (or lost) at the preparation and set-up stage. We believe that attempting to reactively protect fundamentally insecure and ill-designed systems is an expensive and ultimately futile exercise. Reactive security, such as incidence response teams, can only be truly effective on top of a properly executed cyber security strategy that puts secure and layered systems in place.

The state of the art in cyber security technology revolves around proactive security. In proactive security, one aims to build software systems that are fundamentally secure and compartmentalized into isolated parts to limit the effectiveness of any one breach.

The field of software verification has the potential to prove formally that software systems are secure (e.g. a system with no memory vulnerability). This technology has only recently become practical in some settings that are relevant to connected systems and cyber security. Software verification is already used in isolated real-time critical systems (e.g. aircraft computer systems). The next research steps will be to apply software verification to real-time critical systems with limited connectivity (e.g. power plants). In a more distant future, with the advance and spread of this technology, it could become a legal requirement for companies to utilize secure systems (i.e. systems that have been formally verified) for storage of sensitive data (e.g. identity data).

The field of systems and networking has worked for many years on techniques to separate, firewall, and compartmentalize access and data in the presence of breaches. Quite a number of these technologies are already widely used in commodity computing (processes, virtualization, sandboxing), but are often ignored at the higher levels of cyber security strategy.

We believe that the further development of technical fields such as software verification, combined with appropriate separation technologies and cryptography, has the potential to yield highly secure systems that are no longer vulnerable to most of the current cyberattack vectors within the next decade, given the right investments and incentives.

More generally, it is critical for organizations and decision makers to develop a clear understanding of the current technological state-of-the-art, costs, and limitations to create secure software programs, systems, and infrastructures.

Strategy: Managing and Reducing Attack Surfaces

Cyber security can be divided into systems security and data security. While cutting-edge systems technology can help enhance the protection of systems and data, it is also necessary to have a strategy about what data to protect and how to organize it. We identify three principles underlying any data security strategy:

- "It is impossible to secure everything" — Identify the data to secure
- "The most secure data is the data you do not store" – Limit the data to store
- "Don't put all eggs in one basket" — Compartmentalize data

It is impossible to secure everything

The increasing amounts of available data combined with the limitation of resources (computational, financial, organizational, etc) make it impossible to secure all data, no matter how powerful the organization. In this light, the ability to classify data, identify data to secure, and allocate data security resources accordingly, becomes a critical capability. Not all data is equal, its importance depends on the potential damage that its release can cause. Data that is vital for business operations or very sensitive personal data should get the strongest (and most expensive) protection level. On the other hand, ancillary data that

Cyber security can be divided into systems security and data security. While cutting-edge systems technology can help enhance the protection of systems and data, it is also necessary to have a strategy about what data to protect and how to organize it.

is not security critical can have lower (less expensive) security levels, and public data does not need security by definition. Another point to consider is that critical data may become less sensitive over time. For instance, some tactical data goes out of date after a number of years and may no longer require the highest security levels. Therefore, a prerequisite to setting up a cyber security system is to decide which data to secure, with which level of security, and for how long.

Currently, one of the major gaps in this area is the lack of a standard framework and quantitative metrics to help organizations determine which data to secure.

The most secure data is the data you do not store

Another principle to increase data security is to consciously limit the amount of data to store in the first place. In a "Big Data" world where data collection, storage, and processing capacity keeps expanding, organizations and individuals tend to keep more data in their information systems and devices, which in turn increases their exposure and vulnerability to cyberattacks. Every bit of stored data is a potential breach opportunity and therefore carries a cost. In order to reduce risks and costs, one needs to make the conscious effort to store only data that is necessary and not succumb to the temptation of storing more data just because the system has space. Where possible, it is preferable to store data in a temporal, aggregate, anonymized, or incomplete form so that it contains less or no privileged information. An example would be to store online only the last week of diplomatic cables, instead of the full year. Beyond individual organizations and citizens, this principle can guide legal bodies regulating which records must be kept by companies or individuals. While the most secure data is the data that is not stored, record-keeping practices need to comply with the law.

The major challenge in this area is lack of awareness and education of organizations and individuals. At a broader level, this principle also requires legislative bodies to make tradeoffs in the legal framework to balance record-keeping and cyber security needs.

Compartmentalize data

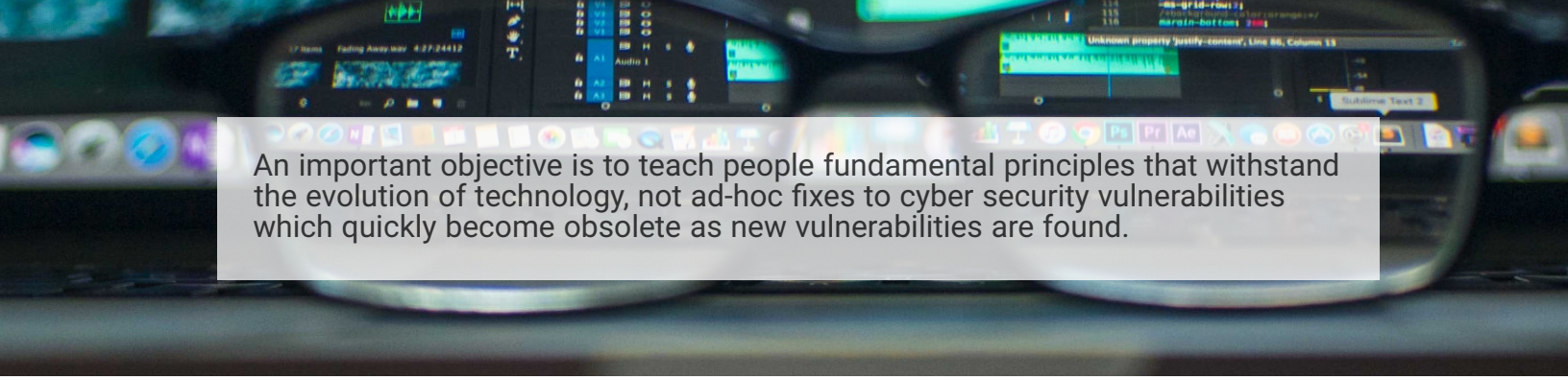
For data that needs to be stored, compartmentalization can help reduce cyber vulnerabilities. As the old saying goes, "don't put all your eggs in one basket". For instance, in the case of customer data, one could store sensitive personal data (e.g. Social Security Number, credit card number, date of birth, etc) in a different database that is more secure than the database used to keep customer shopping history. Because the Internet is a widely accessible place, it is also better not to connect critical data to the Internet, wherever possible, in order to limit the risk of cyber security breaches and the impact of cyberattacks. For instance, one could choose to keep historical diplomatic cables in an offsite physical location that is not connected to any online system. A good practice is therefore to separate confidential data into different compartments (e.g. day-to-day information vs. historical records), each in a different storage location (online vs. offline), with the objective of keeping only the minimum necessary data in widely accessible places.

Human Behaviors: Central Component of Cyber Security

Human behaviors is one of the three pillars of cyber security. Cyber security is ultimately about the security of human beings, who are increasingly connected and thus exposed to cyber risks. Cyber security highlights the inter-connectivity and collective responsibility of all actors in society (international authorities, national governments, businesses, and individual citizens) to create a more secure cyber space.

Raising awareness and further education in cyber security

Knowledge and understanding of cyber security remain largely limited. With the increase of cyber threats, it is critical to raise awareness and educate organizations and citizens about cyber security. Any effective education approach has to include principles, technology, and best practices related to cyber security. If the focus is only on the technology side, human behaviors will remain the weakest link in the cyber security chain. If the focus is only on human users, the learnings will



only have short-term value because technology evolves quickly by its very nature. The objective is to teach people fundamental principles that withstand the evolution of technology, not ad-hoc fixes to cyber security vulnerabilities which quickly become obsolete as new vulnerabilities are found.

Growing a common knowledge base for cyber security

Cyber security is generally very poorly understood, in part because the technological and organizational know-how is still in its infancy. The implications of connecting systems is still in the process of becoming understood, even as the process of connecting systems across the board continues to progress rapidly. The underlying technology is not very new (about 50 years old) but is evolving much faster than previous human periods of technological breakthrough (e.g. Industrial Revolution). As a result, there is no consensus, widely known principles, and guidelines on how to make an information system secure. In contrast, the principles of civil engineering are widely known and accepted. Consequently, improving cyber security and related behaviors requires building the credibility of cyber security as a discipline and foster its development, with objectives and strategies in place that guide how to reach it.

One of the largest gaps in cyber security today is a widely accepted knowledge base for cyber security principles and technologies. Any successful cyber security strategy will require the collection, buildup, and spread of know-how in each key area, at national and international levels. It requires a clear understanding of the current state-of-the-art, costs, limitations, and areas of development for programs, systems, infrastructures, processes, and people. Additionally, policymakers need to continue to find ways to incentivize organizations and individuals to adopt best practices in cyber security. Significant efforts have been done in recent years across nations and organizations, but more remains to be done.

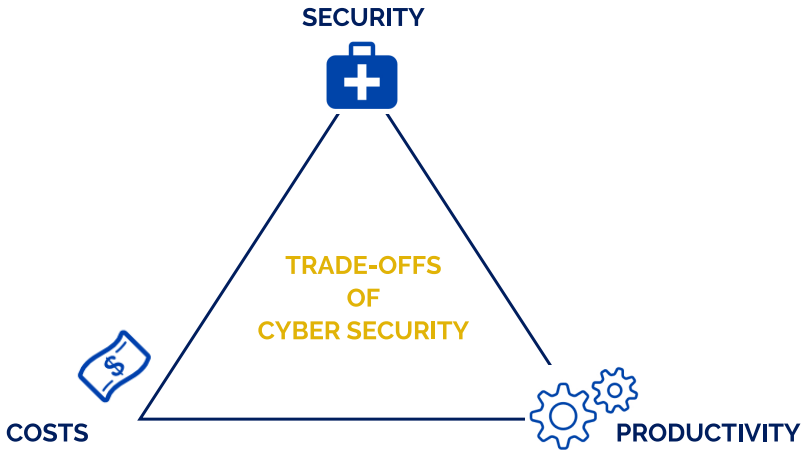
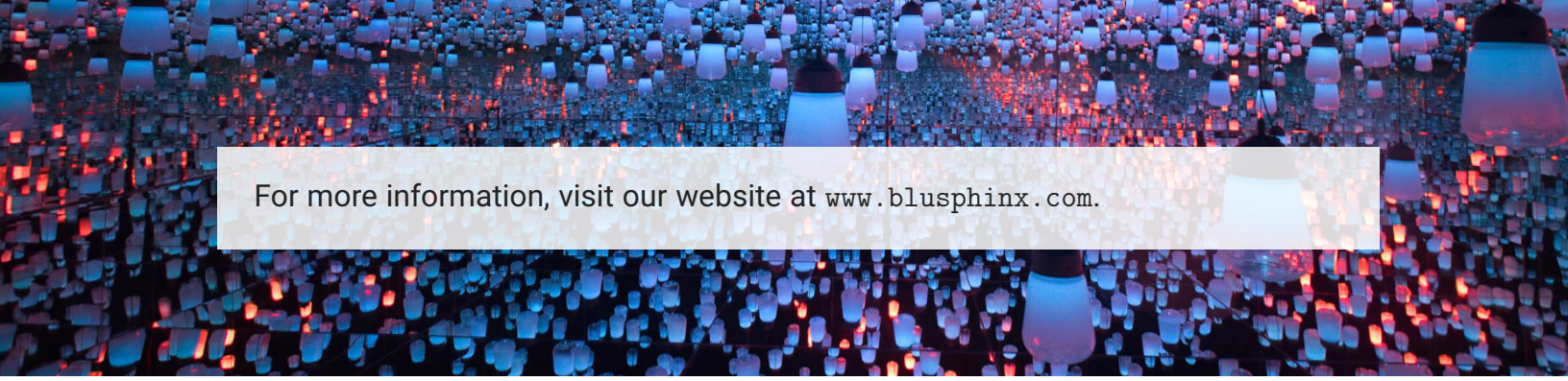


Fig. 3: *The trade-offs between costs, productivity and security.*

Conclusion

Cyber security is a key challenge facing every organization today, and even more so going forward. While there are many inadequate solutions for cyber security, there is no single best solution. To face this challenge, decision makers will need to develop their cyber security strategy, according to their own specific objectives and activities, and make necessary tradeoffs. Cyber security inherently involves tradeoffs between security, costs, and organizational productivity. Security tools come at a cost and the more data is restricted and compartmentalized, the more cumbersome it is to use the data to do work. Different organizations face different priorities and constraints, and must therefore define which tradeoffs are acceptable.

In order to validate trade-offs under attacks, it is crucial to explore one's strategy and choices carefully before a real attack happens. Simulated environments offer a unique opportunity for interactive learning and strategy testing, without incurring the potentially catastrophic cost of real attacks, to determine the appropriate course of action. These learning and testing methods are now crucial to develop central repositories of knowledge and technologies to guide organizations in implementing the best cyber security strategies. They constitute also a cornerstone for the required cyber security training at all lev-



els, from top decision makers to operational teams.

Authors

Thomas Dillig *is a digital engineer and co-founder of BLUSPHINX. He is an expert in computer science, AI, cyber security, software, and project management.*

Aurelie Mei-Hoa Beaumel *is a digital architect and co-founder of BLUSPHINX. She is an expert in digital strategy, AI, data insights, and resilience.*

Gen. (Ret) Jean-Paul Palomeros *is a retired General of the French Army, former Chief of Staff of the French Air Force (2009-2012) and NATO Supreme Allied Commander Transformation (2012-2015).*

BLUSPHINX® is an independent firm of digital architects and engineers. We are experts in getting the most value out of digital technology, while minimizing risks, within constraints such as money, time, or resources. We work with business owners, leaders, and homeowners.

For more information, visit our website: `www.blusphinx.com`

You can contact the authors at `hello@blusphinx.com`.

Bibliography

[1] The New York Times, "Defending Against Hackers Took a Back Seat at Yahoo, Insiders Say." `http://www.nytimes.com/2016/09/29/technology/yahoo-data-breach-hacking.html?_r=0`, September 28, 2016.

[2] The New York Times, "For Target, the Breach Numbers Grow." `http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html`, January 10, 2014.

[3] The New York Times, "F.B.I. Says Little Doubt North Korea Hit Sony." `http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html`, January 7, 2015.

[4] The Washington Post, " OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought." `https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/`, September 23, 2015.

[5] Reuters, "Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat." `http://www.reuters.com/article/us-cyber-heist-philippines-idUSKCN0YA0CH`, May 19, 2016.

[6] ICS-CERT, "Cyber-Attack Against Ukrainian Critical Infrastructure." `https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01`, February 25, 2016.

[7] The New York Times, "Spy Agency Consensus Grows That Russia Hacked D.N.C.." `http://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html`, July 26, 2016.

[8] The New York Times, "Hackers Used New Weapons to Disrupt Major Websites Across U.S.." `http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html`, October 21, 2016.