Digitalization changes the business and the way companies interact with their customers, manage their operations and respond to new competitors entering the market. With this important shift, we are also seeing dramatic changes to, and in some cases a complete disruption of existing business models.

In the wake of these changes, the behavior of people has also changed, forcing businesses to respond. And with more delivery channels available to expand access to markets, we expect companies to integrate their products with new services while leveraging available data to better serve customers in a more transparent way.

All these expected changes call for a transformation of security across the organization and point to companies taking brave steps to elevate their security capabilities to the next level. Most security functions today are driven by a compliance mindset and the key focus for many of these is to make sure all the regulatory policies and regulations are fulfilled. The most popular security practices are in our view no longer effective, efficient and resilient. The security function should become an innovator, with security programs becoming a value-add to the business. It should also treat the business as the “star” to be protected and grown.

With these evolving trends, security functions across the globe should work off new paradigms to create real value-add for the business. Without this refocus, they will remain a form of “insurance policy” for the company, thus limiting their strategic role and ability to effectively guide the business through the challenges ahead.

Key to this is a fundamental mindset shift within a company’s security function. Moving from being a barrier to new business ideas to an active partner in solving “business” problems and supporting the organization’s enhanced adoption of digital technology. For the company, this can mean taking on new opportunities at an acceptable level of risk.

In addition to a new mindset, security functions are also encouraged to embrace a new approach to security management. In this Accenture paper we present such an approach to managing organizational security and explore four concrete initiatives financial services companies can put into practice.
Accenture Security Management Framework

The Accenture Security Management Framework pictured below offers a high level overview of the role of security.

Source: Accenture, July 2016
Putting the Business at the Center

The business is the focal point and center of all directed activities. These activities serve two purposes: protecting the business and enabling it to grow. However, our dynamic environment and emerging trends are making this more challenging and less predictable.

As Accenture’s Technology Vision 2016 report clearly points out, businesses face profound challenges over the next few years because of emerging technology trends. And without a proper risk management approach, these trends cannot be “leveraged” as a platform for creating business value and winning in the digital age. The key trends identified by Accenture include:

**Trend 1: Intelligent Automation**

This is the launching pad for new growth and innovation. Powered by artificial intelligence, the next wave of solutions will help gather unprecedented amounts of data from disparate systems and—by weaving systems, data, and people together—create solutions that fundamentally change the organization, as well as what it does and how it does it.

**Trend 2: Liquid Workforce**

Companies are investing in the tools and technologies they need to keep pace with constant change in the digital era. But a barrier to their efforts and critical factor where they are falling behind is their workforce. Companies need more than the right technology; they need to harness technology to allow the right people to do the right things in an adaptable, change-ready, more responsive and more liquid workforce.

**Trend 3: Platform Economy**

The next wave of disruptive innovation is expected to come from the technology-enabled, platform-driven ecosystems now taking shape across industries. Having strategically harnessed technology to produce digital businesses, many companies are now creating the adaptable, scalable and interconnected platform for an ecosystem-based digital economy.

**Trend 4: Predictable Disruption**

Every business now understands the transformational power of digital. What few have grasped is how dramatic and ongoing the changes arising from new platform-based ecosystems can be. It’s not just business models that can be turned on their heads. As these ecosystems produce powerful, predictable disruption, whole industries and economic segments can be utterly redefined and reinvented.

**Trend 5: Digital Trust**

Pervasive new technologies raise potent new digital risk issues. Without trust, businesses cannot share and use the data that underpins their operations. That is why the most advanced security systems today go well beyond establishing perimeter security and incorporate a powerful commitment to the highest ethical standards for data.

Companies that expect to prosper and win in the digital age have to do much more than simply tick off their technology capabilities list. “Winners will create corporate cultures where technology empowers people to evolve, adapt, and drive change.” In this context, it is key that a company’s security operating model evolves to respond to the new challenges and demands. Within the financial services sector, the Chief Security Officer (CSO) has to play a more active and facilitating role with stronger and closer alignment with innovations inside and outside the organization. We have observed that CSOs who embrace this new mindset are helping to drive innovation within their organization and across the business.
In our new global and digital world, a company's security is dependent upon a broad number of stakeholders. For some financial services security people, employees are potential “security issues” and thus their behavior should be overseen to make sure they do not misbehave.

The needs and expectations of the customer are also changing dramatically in the financial services sector. Even affluent customers want daily and easy access to their funds and information, including greater access to advice online or through unsecure smartphone platforms. Yet, like all customers they continue to expect the same level of confidentiality and availability of data and services.

Adding to the challenge and often underestimated by financial companies are the requirements (e.g., expectations) based on close collaboration with partners in a liquid and flexible workforce enabled by technology. Managing confidentiality, integrity and privacy in such an environment should be simple and transparent.

The security community is also an important stakeholder which should not be underestimated, but often is. Companies are encouraged to clearly spell out how they plan to work with the security community, especially vulnerability finders. There should be a clear strategy and a transparent approach to working with them.

Another important stakeholder are the financial markets as their movements can influence the security needs and architectures of financial services companies. Publicized attacks can influence customers, shape market forces, and define perceptions and feeling for what is good or bad. The same is true of new technologies adopted by the financial services sector and that can alter what people see as acceptable and/or good practice.

Rather, the security function should support employees in their day-to-day activities and tasks as they create value for the business. Technology can help do this in an automated and transparent way.

Our experience indicates that for many companies, senior management understands the role they should play in leading the security agenda, yet they often feel uncertain on the path to follow. Security should become more transparent and in a way that is relevant to a Chief Executive Officer (CEO) and the C-suite. This would facilitate their understanding of the key risks the business faces while encouraging them to act decisively.

The security community is also an important stakeholder which should not be underestimated, but often is. Companies are encouraged to clearly spell out how they plan to work with the security community, especially vulnerability finders. There should be a clear strategy and a transparent approach to working with them.
The “Criminal” Actors

Criminals and attackers also play an important role in a company’s cyber security strategy and approach. Understanding their motivation and mindset is in our view critical to building an effective and efficient security program.

We classify attackers into five categories: vandals, hacktivists, criminals, terrorists and nation-state actors.

Typically, vandals are motivated by reputation and fame. They see hacking as a challenge and opportunity to prove their skills and abilities to peers. Their means are often limited and good security practices should help prevent successful attacks. Companies should expect that threats from vandals remain constant and do not change significantly over time.

As the term implies, hacktivists are attackers whose activities are focused on a political or social agenda. In most cases they have been known to be active in the criminal space or involved with illegal organizations. They tend to have more in common and “share know-how” with criminals and vandals, yet their motivation and goals differ from these criminal elements. Activities among these attackers are expected to remain constant. However, there is a certain likelihood that their attacks might become more sophisticated and unpredictable.

Basically criminals have always been present where the money is. Consequently, their criminal activities followed businesses and their money onto the Internet. Today, there is a fairly significant underground market where services and technology (e.g., purchase of attacking tools such as service level agreements, “rent a hacker,” etc.) are offered and traded among criminals. As this criminal and underground market grows, so does the availability of more and more technology and services which were only available to government agencies and bodies in the past. Unfortunately, as this illegitimate access among criminals grows, defense is getting harder to sustain.

The primary goal of terrorists is to produce widespread fear and destabilize populations and geographic regions through the use of violence and violent acts. They look to create the greatest possible harm and gain the highest possible attention and media coverage. Attacks from terrorist groups are not expected to dramatically increase, however their occurrence should have unpredictable and significant impact on their target while generating considerable collateral damage.

What a nation or state is allowed to do is highly dependent on its laws and regulations as well as the corresponding oversight mechanisms. Attacks by nation-state actors are typically low profile, run over a longer period of time and tend to be sustainable. We expect a significant increase in nation-state attacks with a new level of sophistication. These should become more and more unpredictable and unexpected, requiring greater levels of sophistication in detection.
The Role of the Security Function

The security function has to align its approach to the company’s business strategy, the changing threat landscape as well as emerging technology trends. An interesting and demanding environment in which to operate a security function.

However, according to a study by the Ponemon Institute LLC and Accenture on cyber security and published in 2015, there are companies which are able to reduce the probability of disruption or identity theft by almost 50%.

It is clear, that the security function should take huge and bold steps forward. It should also play a strategic role within the company and become an innovator supporting the business vision. For an effective and strategic function, the focus should be on professional and customer-oriented cyber security with a pro-active approach in the areas of protection, detection, response and recovery.

Technologies like digital and the cloud can help provide great opportunities to move the business in this new direction, if approached correctly. Historical approaches like a strong focus on compliance should prove insufficient in a changing threat and business landscape. As we have seen in the proposed framework, the security function needs to adapt and respond to all the different trends, stakeholders and challenges.

In using cloud and digital to help drive security forward, the following key initiatives should be considered:

- Transforming security
- Investing in threat intelligence
- Building the right identity management program
- Architecting for failure and compliance
From an organizational perspective, security is typically divided into three lines of defense, which are strictly separated. However, to achieve the required change and to be able to satisfy a fast moving business, some organizations combine first and second lines of defense by consolidating policies, governance, architecture, internal consulting, physical security, safety, and even reporting under a CSO, or allocating responsibility between the business CSOs and the technology (security infrastructure) group.

Businesses can take the important steps that follow to transform their security function.

Once the decisions have been implemented, companies should maintain a level of flexibility so as to respond with agility and confidence to unexpected outcomes and situations.

Transforming Security

People are key in transforming security, and as such the effort should be closely led and managed to deliver the desired outcomes. The transformation process should be planned and supported by change management specialists, with a clear signal and a clear start—often this involves the reorganization of the security function.

100-DAY PLAN

1. Define the role of the security function.
2. Define general setup: To drive a substantial transformation, a centralized function should be considered.
3. Define CSO reporting line: The CSO should be considered a strategic role within the company. The CSO needs decision-making authority and the "power to act" within the organization.
4. Define the CSO function.
5. Define key guiding principles such as:
   - How security helps drive innovation
   - How security is a value-add for the business
   - Assume the company is already compromised: Assume the attacker is already in the company’s network
Advanced technologies, like advanced data analytics, put in the hands of skilled resources such as big data people and data scientists, should be considered.

The following identifies important steps businesses can take to invest in their threat intelligence over a shorter and longer time horizon.

Investing in Threat Intelligence

Detection is the new protection. This is where the greatest impact can be generated for the most reasonable investment. Our experience shows that deploying a technology like Security Information and Event Management (SIEM) is not a silver bullet, and depending upon a company’s situation may not be a desirable path to follow.

100-DAY PLAN

1. Understand the company’s assets and business processes. Decide on stable processes to implement (with more or less static use cases) and key focus areas where the business is both highly dynamic and stable.

2. Define a strategy for addressing the static processes either using a classical SIEM or based upon an existing log management infrastructure like the one offered by Splunk Inc.

3. Run a proof of concept using Accenture’s Cyber Intelligence Platform. With this platform companies can work on a pay per use basis. To support the initiative, we recommend assigning an experienced cyber intelligence person to the effort.

4. Following the proof of concept results, decide on the next steps to follow.

   1. Extend the SIEM platform using the Accenture Cyber Intelligence Platform.
   2. Leverage the intelligence to help answer questions specific to the attack: “Who did it?”; “Why did they do it?”; “Why now?”; and “What’s next?”.
   3. Conduct regular training with senior management to help them better understand these three key areas:
      a. How the threat landscape is evolving across the financial services sector
      b. How the evolving threat landscape is affecting the business
      c. How the situation is impacting the company’s business strategy and its security architecture

360-DAY PLAN
Building the Right Identity Management Program

Of major concern to companies, identity management is the foundation for an effective cyber security program. For example, without it, little is gained from encryption if you cannot identify who is accessing the encryption key, or why invest in a firewall if the standard or default password is being used.

Identity management should be addressed from a process and technology perspective. As well, with new and evolving challenges just around the corner, and more and more devices connected to a company’s network, the need to get identity management right becomes quite clear.

The following outlines important steps businesses can take around their identity management over a shorter and longer time horizon.

100-DAY PLAN

1. Conduct an assessment of the company’s current identity management to validate if the organization has the proper setup, governance, processes and tools to support and defend the business. Companies should also define their Identity Access Management (IAM) strategy.

2. Cloud and digital technologies can change a company’s identity story as can the increased use of liquid workforce. Companies should build a cloud-based identity framework and service which can be used by internal services.

3. Establish an Enterprise IAM framework with standards for Business-to-Enterprise (B2E) and Business-to-Consumer (B2C). Tap into new trends like the “Internet of Things” as everyday objects will eventually be connected to networks and will need an identity.

4. Look into the company’s IT strategy and consider using a hybrid IT model and define a vision for a hybrid IAM.

5. Identity federation and the application programming interface (API) economy – externalize what you can and establish specialized services where needed.

6. Create a strategic roadmap.

360-DAY PLAN

1. Unless the company is a single stack shop, review current tooling to validate if this can be sourced more cost effectively.

2. Consider a new sourcing strategy for capabilities, assets and resources. Look for a strategic partner that could deliver these more cost effectively and at a higher quality level.

3. Implement a strategic roadmap and re-assess it constantly as the business and technology will evolve over time.
Architecting for Failure and Compliance

Companies are encouraged to build an architecture which is resilient to attacks and outages. What this means in practical terms is plan for failure. This involves transforming the architecture patterns and blueprints to embed resilience, security and compliance through automated and modular elements.

In so doing, the network is protected and will remain operational in the event of an element failure. Companies should also take steps to update the security architecture for cloud technologies such as containers (e.g., Docker, Inc.).

The following important steps can help businesses transform their architecture over a shorter and longer time horizon.

100-DAY PLAN

1. Define the key guiding principles for the company’s architecture.
2. As a platform, cloud technology offers greater elasticity and resilience and at a lower cost. Companies should consider using cloud as the key infrastructure for running their business in the future.
3. Assess the company’s current situation to get a better understanding of the challenges and issues that need to be addressed during the journey to the cloud.
4. Define a cloud architecture by taking into consideration the principles on failure and compliance.
5. Setup a cloud program.

360-DAY PLAN

1. Run proof of concepts to get a better understanding of possible issues and challenges when completing the actual migration to the cloud.
2. Respond to the issues and challenges identified and implement accordingly.
Conclusion

The Accenture framework discussed in this document outlines clearly the need to transform the security function, and program and leapfrog into the next generation of cyber security management.

In our view this change is critical to supporting digital disruption within the business and benefiting from cloud infrastructures. CSOs in close collaboration with the company’s senior management are encouraged to implement a security change program built on the following key initiatives:

- Transforming security
- Investing in threat intelligence
- Building the right identity management program
- Architecting for failure and compliance

By adopting this new approach, coupled with a new mindset focused on innovation and turning the security function into an active business partner, financial services companies can better position themselves to protect the business and support future growth.
About the Authors

Roger Halbheer
Roger is a Managing Director, Accenture Financial Services Technology Advisory. Based in Zurich, Roger is responsible for the Resilience, Security and Regulatory Technology group within the Accenture Financial Services practice. He brings nearly 20 years of deep and broad industry and consulting experience in the technology, information management and security space. A trusted advisor to C-suite executives and senior public officials on matters of security, governance and information technology, Roger is also a regular speaker at industry events and forums.

Maurice Bollag
Maurice is a Senior Manager, Accenture Financial Services Technology Advisory. Based in Zurich, he brings 15 years of industry and consulting experience across Europe in the areas of security, IT risk, IT advisory, digital identity and access management. His current focus is working with high profile banking, insurance and capital markets clients in the areas of IT resilience, cyber security and regulation technology.

Richard Hösl
Richard is a Senior Manager, Accenture Operations, Security & Risk Services. Based in Munich he leads the Accenture Digital Identity team in Austria, Switzerland and Germany providing integrated services for compliance-driven enterprises in financial services as well as customer-centric organizations. He brings over 15 years of deep experience from across industries in the area of identity access management strategy and planning and the implementation of emerging technologies.

References
2 Ibid

About Accenture
Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 384,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.