Cybersecurity: moving from anchor to enabler of innovation

Insights on governance, risk and compliance
Disruption is unleashing value — but also new risks
The digital and FinTech-driven disruption and transformation of financial services continues – but at what price?

Today, technology-driven innovation is transforming financial services (FS) – enabling firms to create new products and services, enhance access and experiences for customers, strengthen controls and drive down costs. As banks and other financial services firms define their digital strategies, their operations are becoming ever more integrated into an evolving and at times poorly understood cyber environment: a connected ecosystem of entities, people, machines and data, where mobile and social channels are increasingly used to conduct transactions that touch core financial systems.

This means organizational perimeters are quickly disappearing. So, we’ve succeeded in opening up new avenues of cost-saving, agility and speed-to-market. But at what price?

This question is important – because confidence and trust in financial services firms and their offerings depend critically on robust assurance that transactions, data and systems are safe to use and secure, protect users’ information and have integrity. But digital transformation, while vital to maintaining relevance with today’s customers, introduces new risks and potential weaknesses for institutions looking to innovate. Jumping head-first into the digital “deep end” without sufficient focus on cybersecurity adds a level of risk that traditional teams and methodologies may be ill-equipped to address.

**Striking the right balance between regulation, privacy, digital and cybersecurity**

Furthermore, building value successfully in the digital domain in financial services demands a fine balance between regulation, privacy, digital and cybersecurity. And a focus on preventing cyber threats has at times delayed or impacted firms’ digital innovation efforts.

This is one reason why cybersecurity – rightly or wrongly – has at times been seen as drag on digital innovation. For firms to turn it into a positive enabler, they first need to check that they are striking the right balance between regulation, privacy, digital and cybersecurity when designing and developing new services.
Section 1

The digital and FinTech-driven disruption and transformation of financial services continue – but at what price?

Cybersecurity must be integrated into digital innovation teams ...

How can they achieve this? A vital step is to close the current gap between digital and cyber teams, which often effectively operate as separate functions. Digital teams tend to be quite clearly defined and delineated, as opposed to being integrated with cyber capabilities in the up-front visioning and design phases. Cyber skills are then brought in as needed through toll gate-type reviews.

This separation undermines the value of the combined functions. Effective and embedded cybersecurity is the bedrock of any successful strategy for creating value from digital. In a study by Cisco1, 69% of executives indicated that they “are reluctant to innovate in areas such as digital products and services because of the perceived cybersecurity risks.” Such findings underline that uncoupling digital development from cybersecurity risks impeding firms’ growth in the digital space.

… to realize digital value in a FinTech-disrupted world

To avoid this risk, financial services organizations should embed cybersecurity resources into their digital teams. By doing this, they will gain the ability not only to reduce cycle times by designing security from the start, but also to generate higher value, by shifting the core rationale for cybersecurity from preventing breaches to enabling innovation and growth. Closing the gap between cybersecurity and digital will also put firms in a better position to defend their offerings against cyber threats and become trusted digital providers with their customers – an increasingly vital status amid today’s FinTech-led disruption and competition.

As highlighted in a recent EY research report, the global FinTech industry is growing apace, using technology innovation to capture market share in many areas of financial services.2 So the traditional financial services business model is being challenged where it matters most: with customers. EY’s FinTech Adoption Index, based on a survey of more than 10,000 individuals in six countries, shows that 33.1% of digitally active consumers in New York have used at least two FinTech products in the past six months3 – the highest figure in any urban center in the study.

The opportunities and challenges for FS firms

This shifting digital landscape presents substantial opportunities for FS firms. But they can only realize these opportunities if their digital services are underpinned by robust and pervasive cybersecurity – which means it should be built in at the beginning, not bolted on as an afterthought. For those firms that succeed in developing digitally enabled customer offerings that are compelling, relevant, user-friendly and secure, the prize on offer includes new and more profitable products and services, new economic models, and the ability to engage more intimately and regularly with consumers across multiple channels.

But for many financial services incumbents, winning this prize means overcoming some significant hurdles. Their existing core systems infrastructure – often built up through years of legacy architectures, add-ons and workarounds – may lack the agility to adapt quickly to new engagement models and a single, omnichannel, real-time view of the customer. But often, the biggest hurdle to realizing digital value is culture. To drive customer-focused innovation, firms need people with high digital IQs who are adept at working across multiple disciplines and applying new approaches. This means moving toward a controlled “fail-fast-and-move-on” culture, and using techniques such as design thinking, customer-centered journey mapping, DevOps and new design/development methods.

To make this change, financial services firms must move away from a low tolerance to all risks and adopt an approach based on truly understanding risks, thinking through appropriate mitigations, and being confident in their decision-making. This involves a shift in culture toward accepting a controlled failure as “normal” when defining and refining solutions, because more prototypes will get thrown in the trash than make it to market. Such a mindset may not fit easily with the embedded risk-averse culture – and this is one reason why many financial services firms are establishing global innovation hubs with their own distinct culture, resourcing and incentives.
Trust is the bedrock of FS — and digital offerings must foster trust, not erode it.
Section 2

Customer needs are driving innovation and disruption

Consumers’ rapid adoption of disruptive FinTech offerings reflects the way these solutions combine transparency, capability and personalization to meet customers’ needs on their own terms — thus building trust with customers in ways that financial services firms have not previously achieved. Customer trust is the foundation of any financial services firm’s ability to operate, and it’s vital that nothing — including a lapse in cybersecurity — is allowed to undermine that trust.

This heightened customer focus on cybersecurity is occurring at a time when commercial customers are embracing consumer-focused digital innovation for their personal use, and seeking services that provide similar functionality, capability and user experience in their work context. This shift means that customers will increasingly refuse to do business with a financial services provider that fails to offer a top-of-the-line user experience, underpinned by effective yet seamless security that they feel confident will protect them online.

To provide such an experience, incumbent financial services companies must apply innovation to adapt, disrupt and reinvent their offerings and operations in ways that combine the right blend of functionality, ease of use and cybersecurity. Firms across the industry are rising to the challenge by harnessing digital to drive transformation and new business models, powered by advances in devices, channels, data, and platforms such as cloud and the Internet of Things (IoT). By leveraging these innovations, financial services business are seeking to keep themselves relevant to their customers, create new value and build digital trust. These efforts include rising investments in new digital products as well as front- and back-office operations, together with innovation programs in areas such as blockchain, robotics and augmented reality.

The ultimate goal is to provide an intuitive and transparent yet secure experience that builds digital trust among customers, thus supporting the wider trust on which the business depends. Firms that achieve this can make digital trust an integral part of their value proposition — an opportunity that further underlines why cybersecurity needs to be embedded into digital innovation. Financial services companies seeking to build deep digital trust can draw some valuable lessons from e-commerce players (see information panel). Firms should also pay close attention to the ongoing convergence between security and privacy now being driven by regulatory initiatives such as the European Union’s General Data Protection Regulation (GDPR). The maturity levels around privacy vary widely between geographies — and concerns over privacy are a major driver of government intervention and regulation, especially in developing economies striving to catch up with more mature jurisdictions.

Learning from e-commerce: creating digital trust with consumers takes more than an SSL certificate

Online retailers grow consumer trust by providing tools to help shoppers make good decisions, engaging in persistent, active social conversations with their customers, and providing as much transparency as possible around things such as pricing and cost. Smart retailers understand that in order to win in the marketplace, they need to anticipate and then meet consumers’ needs even before consumers themselves have become aware of them. This requires advanced personalization techniques that meet today’s regulations and expectations around privacy, and depend critically on “opt-in” permission from their customers to share their data. All of this presents potentially valuable lessons for financial services firms.
Section 2

Customer needs are driving innovation and disruption

Technology can cut both ways
While the opportunities in areas such as digital trust underline the benefits that technology can bring to financial services firms, it’s important to grasp that technology can be a double-edged sword. All technologies have inherent weaknesses that may become more apparent as complexity grows and the availability of processing power expands. And as institutions digitize increasing amounts of their customer-facing processes and tools, significant amounts of new technologies and interactions are being introduced, each with their own weaknesses to be exploited. When these technologies are presented on enterprise and global scales, the potential attack surface grows exponentially.

So, amid the hype, organizations shouldn’t put too much faith in the “next big thing,” be it encryption, biometrics, robotic process automation or blockchain. Crucially, many of the benefits technology offers to enterprises – such as the massive processing power of the cloud – are also accessible to criminals. Organizations that successfully introduce these cutting-edge technologies need to infuse cybersecurity concepts and practices through their entire development life cycle, in order to identity and mitigate these new risks as part of their innovation process.

Once again, these are important messages that cybersecurity specialists are uniquely placed to communicate to the business. And as technology advances, cybersecurity risks also change and evolve – potentially raising challenges for existing ways of mitigating risks. Take encryption: throw enough processing power at it, and any encryption system can eventually be broken. With the advent of commercially available quantum computing, the days of encryption may be numbered. Another risk is what the Information Security Forum (ISF) calls “opaque algorithms.” In its Threat Horizon 2019 report, the ISF highlights how companies’ use of algorithms to make decisions in critical systems means they have less visibility into how their systems function and interact, creating a lack of transparency that poses information security risks.4

A mindset focused on opportunities – not barriers
Positioning cybersecurity as a business enabler

We've described an environment in which financial services firms are driving digital innovation, continuing to build digital trust with customers and becoming increasingly enmeshed into digital ecosystems. However, as they take these positive steps, the daily drip-feed of media stories about cyber breaches is a constant worry. Senior executives in financial services are all too aware that their organizations are targets of cyber adversaries ranging from nation state-backed attackers to terrorists, and from hacktivists to organized criminals.

The ongoing proliferation of cyber threats has fed into a belief among CIOs across all industries that their cyber defenses are inadequate. EY’s 19th Global Information Security Survey 2016-17 – *Path to cyber resilience: Sense, resist, react* – finds that 86% of CIOs surveyed say their cybersecurity function does not fully meet their organization’s needs. This figure is down only slightly from 88% the previous year. The report comments: “Despite the steps organizations have taken, it is still not enough to deal with the worsening situation.” What’s clear is that the threats are real and growing – and that the question is how to address them.

### Switching from a reactive stance...

This blend of deep concerns and fast-expanding threats puts us at a defining moment – one where cybersecurity professionals have a golden opportunity to step up and save the day. But this is proving difficult to achieve in practice. Digital development projects involving a cybersecurity layer often expose a stark contrast between the pace and agility of the digital component and the slower-moving and more rigid methodology on the cyber side. Instead of being on the front foot, the cybersecurity community is back on its heels and remaining largely reactive in its stance.

It’s probably fair to say that as digital innovation forges ahead, cybersecurity as a discipline is lagging behind. This failure to keep pace with the advance of digital reflects two problems. First, the traditional thinking, approach and organizational structures around cybersecurity are not evolving quickly enough. And second, in financial services especially, the cybersecurity function is at times left standing on the sidelines, watching the rapid digital transformation that is underway at an enterprise level.

### ...to proactively riding the innovation wave

So, what can cybersecurity do to get more involved, support innovation more effectively and proactively, and start to ride the digital wave? A number of things – all centered around closing the gap with digital. Three steps to achieve this are set out in the accompanying information panel.

---

Three steps to close the gap between digital and cyber teams:

- Embed cyber skills in digital development teams from day one, rather than having them organized in a separate silo
- Enable and empower cyber specialists to apply new methodologies in design and development
- Encourage the adoption by the cyber team of a controlled, carefully managed “fail-fast” culture in the development and prototyping stages

---

Section 3
Positioning cybersecurity as a business enabler

However, our experience shows that efforts to embed cybersecurity into digital development teams often come up against resistance from cybersecurity professionals themselves. This generally reflects their understandable concern that focusing more on the opportunities and business outcomes of digital innovation could cause the organization to lower its guard and risk more cyberattacks succeeding. The resulting divide between digital and cybersecurity can strengthen the feeling among CIOs that the cybersecurity function is not fully meeting their organization’s needs, as noted by the ISF.6

However — more positively — EY research confirms that as financial institutions look to bring digital and cyber together, cybersecurity vigilance remains top of mind. EY’s seventh annual global EY/IIF bank risk management survey, A set of blueprints for success — based on interviews with 67 banks from 29 countries — finds that cybersecurity risk ranks second only to regulation on the entire risk agenda for respondents’ boards (see Exhibit 1).7 Also, 89% of interviewees say cybersecurity is now subject to a particular or enhanced focus on operational risk, more than for any other area of the business.

Exhibit 1: Top three risk areas for boards of directors in the next 12 months
Source: A set of blueprints for success: Seventh annual global EY/IIF bank risk management survey, 2016

---

A new model emerges for cybersecurity

Overall, the message is clear: cybersecurity presents clear and growing risks in financial services – and efforts to tackle these are lagging behind the rapid advance of digital solutions. But the good news is that modern cybersecurity can and should seize the chance to close the gap with digital and ride the wave of innovation and opportunity.

Whatever its current challenges, the cybersecurity field has great technology and highly skilled people. To realize their collective potential and target it more effectively, what’s needed is a new sense of urgency and direction to integrate cybersecurity professionals more closely with their digital colleagues, and energize and inspire them to do things differently. At the same time, the cybersecurity discipline should be expanded beyond protecting the organization against threats, to include a “detect and respond” mindset.

For this approach to work, it will require new philosophies. These include distributing responsibility for security much more broadly – so it’s embedded (like digital) in the business rather than being in a separate silo. Cybersecurity professionals should also become better risk practitioners, working with operations and technology risk specialists to quantify risk more accurately.

All of this will allow people with more diverse perspectives to participate in decision-making around cybersecurity, leading to better and more holistic outcomes. To maximize the benefits, cybersecurity specialists should also move to more nuanced and proportionate approach to risk, and work hand-in-hand with digital colleagues to apply new, more experimental methodologies that balance the twin goals of securing technologies and data on the one hand and realizing business benefits on the other.
The future of cybersecurity: not a brake on innovation, but an accelerator of value
Preventing for cybersecurity's future as a driver of innovation and growth

At some of our most advanced clients, we can already see the future of cybersecurity emerging, with a clear shift underway from old defense-centered thinking to new models focused on enablement. Companies used to look at their innovative digital products under development and ask, “How can we secure them?” Now they’re asking: “How can these products be used to secure our business, and grow our customer trust and revenues?”

This shift of mindset from thinking about cybersecurity as a cost of doing business to seeing it as a growth enabler is not easy. For many firms, it represents a cultural and organizational sea change — one that some cybersecurity specialists understandably resist on the basis that it could increase vulnerability to attacks.

But our view is that this is a change that firms must embrace — and that those that do so will be well-placed to become leaders in financial services as its digital transformation continues. Indeed, as forward-looking firms bring cybersecurity together with their digital teams and the wider business, the question may arise of whether cybersecurity as a distinct function should disappear and become completely embedded into the business. This may happen in some organizations – but cybersecurity-specific skills and information-sharing networks will still be needed, and will remain critical to stay ahead of the advancing threats.

Whatever organizational structure is chosen, our experience with clients suggests that the blend that brings the greatest confidence is a mix of business and technical skills often termed “suits and jeans.” And it’s clear that firms that feel more confident in their ability to manage cybersecurity risks are more likely to innovate and invest in mission-critical initiatives.

With this in mind, companies should ask themselves a number of searching questions about their current and future approaches to cybersecurity, such as:

• Is cybersecurity part of your value proposition, and how can it play a positive role in growing revenue and market share?
• Are your digital development teams both digital-savvy and cyber-savvy? How about your executives?
• Is your cybersecurity organization seen as a business enabler or a blocker?
• Have you considered rethinking your new digital processes with cybersecurity as the foundation from the ground up?
• Are you applying new digital governance models suited to operating in the face of growing cyber threats?

The answers to such questions will help guide your organization toward the future of cybersecurity in financial services – as a proactive enabler and facilitator of digital growth, innovation and trust.
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EY is a leader in serving the global financial services marketplace

Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY’s Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY’s financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

© 2017 Ernst & Young LLP. All Rights Reserved.

EYG No. 02018-171Gbl
1703-2218875 BDFSO
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com