HOW BANKS DRIVE DIGITAL TRANSFORMATION FORWARD

Empower Innovation & Manage Risks with a Team Approach

SAFEGUARD CYBER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

90% of financial services firms have commenced their digital transformation initiatives.[1] What do businesses need to do to ensure their strategies are successful without compromising on security?

Mobile banking is one of the top three most used apps for US consumers[2]

Customers are more likely to interact with banks online than any other channel[3]

Approximately 64% of US consumers rely on digital banking services[4]

Few industries have seen as much disruption as retail banking in recent years. Many once well-established banks are finding themselves under increasing pressure to modernize as more agile startups threaten to usurp them. Today, almost two thirds of US consumers rely on digital banking in some form, with mobile being a favorite channel. More conservative organizations are rapidly falling out of favor as consumers choose banks focused on delivering more convenient digital experiences.

These changing consumer habits are the driving force behind digital transformation in the banking sector. Consumers now look to social media for updates on service status and instantaneous customer support. They're using smartphones to pay for groceries at the local supermarket, and they're using mobile authentication apps to safely enjoy all the benefits digital banking has to offer.

Behind these experiences are teams for marketing, compliance, security, customer support, and product development, to name a few. Delivering the user experiences that consumers demand requires these teams to work effectively together. That's where modern technology comes in to enable a more collaborative and agile workforce:

Social media enables faster customer care and brand connection.

Collaboration tools empower corporate teams to work more efficiently across multiple offices, branches, and time zones.

Mobile chat powers quick and convenient conversations.

Cloud productivity suites like Office 365 reduce in-house technology costs and give employees the freedom to work online.

As with all new technology, these channels also come with security and reputational risks. However, choosing to ignore them cedes market share to more nimble competitors. Driving the adoption of digital channels can pose a monumental challenge for enterprise organizations, which tend to be more siloed. That's why the only way to implement transformative digital technologies effectively is to coordinate between teams and break down the information silos that lead to widespread confusion over who's responsible for security and brand reputation management.

WEIGHING THE RISKS & OPPORTUNITIES OF NEW DIGITAL TECHNOLOGIES

AI is expected to save the banking industry $1 trillion in the US alone[5]

75% of banks are investing in developing customer-centric business models[6]

80% of bankers see open banking as a strategic opportunity[7]

More than ever, consumers are demanding rich omnichannel user experiences; ones that don't force them to spend half an hour on the phone when they've forgotten their online banking credentials or use a desktop web browser to check their balances. Consumers are craving an ever-wider range of features and communication channels but, at the same time, security remains their number one concern. There's a rock-solid reason for that too – banks are 300 times more likely to be targeted than businesses in other industries.[8]

Digital risk isn't just restricted to cyberattacks. There are other factors, such as human error, failing technology, and accidental data loss to think about too. Here are some of the most common digital risks for today's banks:

MALWARE ATTACKS

Malware assumes many forms and takes advantage of a great variety of attack vectors, from social engineering scams to software vulnerabilities. Common types of malware include adware, spyware, viruses, trojans, and ransomware. The latter has recently become one of the more popular types of malware.

PHISHING SCAMS

Cybercriminals are always looking for the path of least resistance. It can take less time to hack a human's trust than a well-engineered network. As such, the human element is usually the weakest link, hence the ubiquity of social engineering scams. By posing as members of a legitimate company, or even as friends or colleagues, scammers attempt to dupe victims into unwittingly surrendering confidential information.

VIP ATTACKS

Smarter and more resourceful scammers often target high-profile executives rather than carry out simple phishing scams en-masse. These so-called spear-phishing or 'whaling' campaigns involve intensive research into the intended victim for the purpose of customizing the attack. In other cases, scammers may impersonate executives to increase their chances of duping lower-ranking employees.

REPUTATIONAL RISK

Digital sabotage remains a serious problem in an age when cyberwarfare conducted by foreign states routinely targets influential organizations, such as high-profile banks. However, given how quickly information (or misinformation) spreads online, even one angry customer taking to social media to voice their complaints can be enough to result in serious damage to a brand's reputation.

DATA LOSS

Not all cases of data loss are a direct result of malicious actors. In siloed organizations where there are no established protocols for exchanging information, there's a much higher chance of sensitive data being accidentally disclosed. Not only does data loss present serious operational and productivity problems – it can also lead to a breach of data privacy regulations.

COMPLIANCE FAILURES

In an industry where trust is everything, it comes as no surprise that banks are subject to a wide range of regulations. A lack of oversight of digital communications is bound to lead to compliance violations resulting in harsh penalties. With that comes potentially enormous reputational damage, as well as the high costs of litigation, remediation and recovery.

How can the banking sector adopt a digital transformation strategy that overcomes security and reputational challenges?

The answer is a team-driven approach built on the understanding that these challenges are everyone's responsibility.

CYBERSECURITY – WHO'S PROTECTING WHAT?

81% of consumers who pay bills online cite personal data and identity theft as one of their greatest concerns.[9] Yet, despite these concerns, they're still craving more mobile banking features than ever before.

Both the transformative power and the risks associated with new digital technologies stem from the fact that these critical channels lie outside of network perimeter defenses. On social media, for example, it can be difficult for marketing-oriented community managers to recognize the signatures of spear-phishing or account take over attacks. Moreover, employees posting on their own social media accounts may be vulnerable to targeted social engineering attacks, threats that are completely invisible to the enterprise.

Even collaboration channels which are ostensibly for "internal" communications, like Slack or Yammer, present unique challenges. As cloud-based applications, malicious content or malware links remain difficult to mitigate for traditional network controls.

CRITICAL CHANNELS LIE OUTSIDE OF NETWORK PERIMETER DEFENSES

To mitigate these risks, administrators need to maintain complete visibility into digital assets like social media accounts, instant messages, and any other branded communications and properties. Furthermore, security teams need access to real-time threat intelligence. They require the ability to communicate and work with marketing and compliance teams quickly to coordinate remediation efforts. Alerts are not enough, security tools must be able to lock down accounts that are being misused, quarantine threats, and close compromised or impersonated accounts.

With a centralized monitoring and control system, security teams have real-time visibility into all information being posted online from owned channels such as social media profiles and instant messages. Instead of trying to secure information at the device-level, such a defense system extends perimeter defenses around cloud-based digital channels, enabling banks to protect critical information assets and business operations.

MARKETING – THE NEW FRONTLINE IN BRAND DEFENSE

59% of consumers claim that they will not hesitate to stop doing business with a bank that suffers a data breach.[10] Thus, reputational damage is one of the biggest costs resulting from a data breach.

Traditionally, digital security has always been seen as something only IT departments have to worry about. However, given widespread use of digital channels throughout every department, it's now safe to say that marketing and customer-relationship teams are the new frontlines in brand defense. After all, it can take many years to build up a solid reputation, but mere seconds for just one malicious action to undo everything. The Marketing Accountability Standards Board has found that brand value contributes about 19% of enterprise value, research corroborated by the Forbes Marketing Accountability project.[11] Fake or fraudulent accounts that damage brand reputation can, therefore, have a measurable dollar impact on a company's stock price or value.

Hackers routinely target banks using social media, which is what happened when criminals set up fake Twitter accounts to direct Bank of America customers to fraudulent websites designed to steal credentials back in 2015. Moreover, a recent North Korean operation leveraged a LinkedIn job posting to hook a developer working at Chile's Redbanc ATM network.[12] With brand impersonations being one of the biggest threats to banking, CMOs must work more closely with CISOs as brand reputation risks and cyber threats are now intertwined.

By eliminating the widespread corporate confusion as to who is responsible for social media security, for example, banks can extend the culture of accountability to their marketing teams as well.

CMOS MUST WORK MORE CLOSELY WITH CISOS AS BRAND REPUTATION RISKS AND CYBER THREATS ARE NOW INTERTWINED.

While CISOs may be responsible for selecting and implementing the right technological and administrative controls, CMOs must be responsible for ensuring that their teams communicate reputation risks, such as fake or imposter accounts, to security teams for remediation.

GOVERNANCE – A CHANCE TO GAIN BUSINESS INSIGHTS

Banks are already spending $270 billion on compliance-related costs every year, but a sizable portion of this is a direct result of corporate confusion as to who's responsible for things like communications on social media. [13]

Regulatory compliance isn't just bureaucracy – it's a direct and highly necessary result of the fact that digital safety and privacy are squarely at the forefront of consumers' minds. In no case is this truer than banking, in which few people would continue doing business with a financial institution that doesn't have an impeccable track record when it comes to protecting consumer data.

Compliance-related issues are magnified on a massive scale with the use of social media and mobile chat technologies in the banking sector. Larger banks have hundreds of employees posting on multiple platforms multiple times per day. Promissory language and exposure of sensitive or misleading information, whether intentional or accidental, can all lead to serious compliance violations.

COMPLIANCE-RELATED ISSUES ARE MAGNIFIED ON A MASSIVE SCALE WITH THE USE OF SOCIAL MEDIA AND MOBILE CHAT TECHNOLOGIES IN THE BANKING SECTOR.

However, simply refusing to engage with new technology, or outright forbidding employees from using these channels is unrealistic. Fear is not a sustainable business strategy. Whether it's incentive structures or a market imperatives, employees will gravitate toward tools that make their jobs easier or more profitable. With this in mind, compliance and risk teams should look for ways to enable and empower their workforce to use these new digital tools securely. Moreover, there is a hidden business opportunity. Automated archiving provides a more actionable data set. By simplifying capture and compliance protocols, an organization frees up time to better analyze what is being captured. In these messages, which before were seen as a compliance risk, may lie key business insights about opportunities for new products or services. In this way, data protection also becomes data enablement.

MITIGATING DIGITAL RISKS WITH A TEAM-DRIVEN APPROACH TO TRANSFORMATION

When one considers the sheer scale of digital communications in today's enterprise environments, it's easy to dismiss it as an impossible struggle at first. In the case of banking, it's even more complicated, given the frequent disconnect between different lines of business such as retail banking, wealth management, and insurance. On top of that is the fact that many departments have a different set of procedures, tools, and channels. Add social media and instant messaging into the mix, and the margin for error increases exponentially.

Fortunately, there's a way to deal with the ever-increasing scale of digital in today's banking environment. Armed with automation and real-time detection, administrators will be able to intercept threats and act immediately all while ensuring that their data-governance procedures stay in line with their compliance obligations. This starts with breaking down information silos and developing a team-based approach to address the following key steps:

1. INITIATE A DIGITAL RISK ASSESSMENT

With full support of the CISO, CMOs should conduct a risk assessment of their digital channels to determine the brand's resiliency and balance to quantify risk.

2. MAP THE DIGITAL FOOTPRINT

CMOs should draw up a complete list of all digital communication assets in use across the organization, including social, collaboration, mobile, and internal cloud applications.

3. SURVEY USER ACTIVITY

Using automation technology to overcome the challenges of scale, CISOs should lead the way in confirming channel usage and flagging unauthorized accounts.

4. IDENTIFY VULNERABILITIES

CISOs must thoroughly investigate existing risk exposures, determine and prioritize vulnerabilities, and ascertain optimal channel-coverage requirements.

5. DETERMINE SOLUTION REQUIREMENTS

Both CMOs and CISOs must determine what they need to protect their digital assets, since both are responsible for matching the solution to their operational environments.

6. DEPLOY A RISK-PROTECTION SOLUTION

Once agreeing on a budget and obtaining sign-off from management, CISOs will be in charge of placing digital channels under the governance of a risk-protection solution.

SECURING SOCIAL MEDIA AND OTHER DIGITAL CHANNELS ARE THE OVERLAPPING RESPONSIBILITIES OF CMOS AND CISOS. WITH A TEAM-DRIVEN APPROACH, BANKS CAN CREATE A CULTURE OF ACCOUNTABILITY THAT TRANSCENDS THE LIMITATIONS OF SILOED MANAGEMENT SYSTEMS.

FINAL WORDS

The consumer-banking sector is starting to feel the enormous pressure posed by more innovative competitors that are popping up every year. However, along with the demands for more flexible user experiences and instant gratification are the profound security, compliance, and reputational risks. Consumers want to be empowered to do more with an ever-wider range of features and communication options, but their privacy and security remain their top concerns.

SafeGuard Cyber was built to help enterprises simplify and secure digital transformation at scale, from local credit unions to global financial institutions with millions of customers. By providing complete visibility into 50+ social media and digital channels, our platform empowers teams to use new technology without fear. To achieve this, our solution uses machine-learning and cloud-to-cloud integration to overcome the challenges of scale. Our belief is that cybersecurity isn't just an insurance policy, but an opportunity to innovate and grow your business.

Find out how SafeGuard Cyber is helping banks drive digital transformation by requesting your complimentary risk assessment today.

www.SafeGuardCyber.com/banking

SOURCES

[1] http://www.fujitsu.com/global/about/resources/news/press-releases/2018/0712-02.html
[2] https://www.multivu.com/players/English/8313051-citi-mobile-banking-study-2018/
[3] https://www.pwc.com/us/en/financial-services/publications/assets/pwc-fsi-whitepaper-digital-banking-consumer-survey.pdf
[4] https://www.statista.com/statistics/946104/digital-banking-users-by-generation-usa/
[5] https://next.autonomous.com/augmented-finance-machine-intelligence
[6] https://www.pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf
[7] https://www.temenos.com/en/news-and-events/news/2018/january/8-in-10-bankers-see-open-banking-as-an-opportunity/
[8] https://www.itspmagazine.com/from-the-newsroom/the-cost-of-a-cybersecurity-breach-for-financial-institutions
[9] https://thefinancialbrand.com/74044/mobile-banking-features-digital-security/
[10] https://safenet.gemalto.com/resources/data-protection/data-breaches-customer-loyalty-report-2017/
[11] http://cmo-practice.forbes.com/wp-content/uploads/2017/08/Forbes-Marketing-Accountability-Executive-Summary-10.2.17.pdf
[12]https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/
[13] https://internationalbanker.com/technology/spotlight-compliance-costs-banks-get-business-ai/

SAFEGUARD CYBER

Americas
410A East Main St.
Charlottesville, VA 22902
USA

+1 (800) 974-3515

sales@safeguardcyber.com

Asia-Pacific
PO Box 523
Leichhardt NSW 2040
Australia

+61 (437) 276-739

APACsales@safeguardcyber.com