RSA

WHITE PAPER

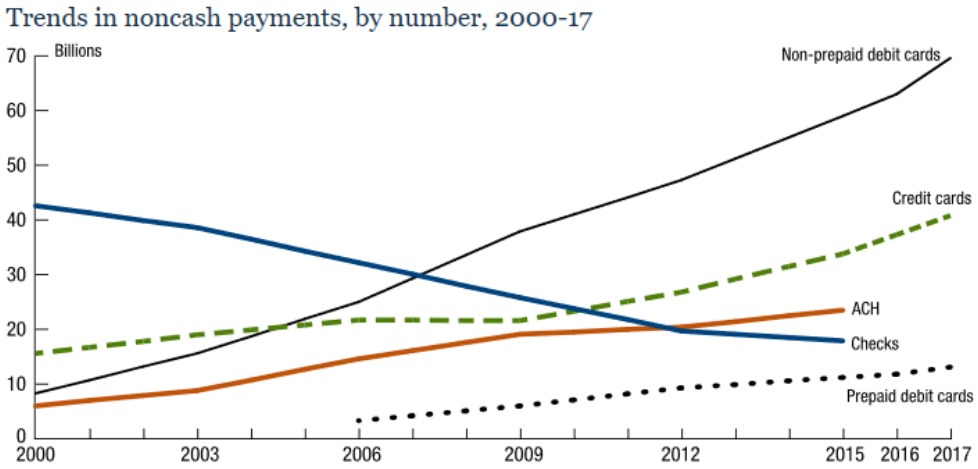
DIGITAL RISK MANAGEMENT IN BANKING

Banks are not new to the concept of digital risk management. Some of the very first digital technology was developed as early as 1939,[1] and banking was likely the first private sector industry to widely apply digital technology to its day-to-day business activities.

A SHORT HISTORY OF SELECTED BANKING TECHNOLOGY

Notable applications of digital technology in banking include the following.

- In 1956, the American Banking Association adopted technology introduced by Bank of America that employed magnetic ink character recognition (MICR) to capture and sort physical checks. This innovation reduced the time to process checks by 80%.[2] This check-processing technology has become universally accepted throughout the banking industry.
- In 1967, Barclay's Bank was the first bank to introduce an automated teller machine (ATM) to dispense cash. Today, there are well over 1.7 million ATMs in use worldwide.[3]
- Cash and checks used to be the sole means by which individuals would pay for the goods and services they received. In the 1950s credit cards were introduced, followed by debit cards in the 1960s and automated clearing house (ACH) payments in the 1970s. Each of these digital innovations dramatically transformed how banks extended credit and disbursed funds from customer accounts, and how businesses disbursed employee payroll (which was once disbursed in cash or check but is now disbursed by ACH credits to employee bank accounts). While these technologies have not yet entirely supplanted the use of cash and checks, they are well on the way to doing so.



Source: Federal Reserve Payments Study: 2018 Annual Supplement, Board of Governors of the Federal Reserve System https://www.federalreserve.gov/paymentsystems/2018-December-The-Federal-Reserve-Payments-Study.htm

Each application of digital technology in banking has created the opportunity to enhance positive customer experience, grow revenue through new and expanded services, and process transactions more efficiently, effectively and at lower cost. However, with every opportunity digital technology has provided to banks, customers and counterparties, it has also transformed existing risk and often introduced new risk.

- The application of MICR to automate check processing dramatically increased the speed of check processing and significantly freed up human resources, increasing revenue and reducing expenses. By carefully choosing the route checks would take to settle, banks increased revenue by speeding up the availability of customer check deposits and delaying the clearing of customer check payments. Manipulating check routing allowed banks to use customer monies for longer durations, providing banks with more funds on which they could generate interest income.

  The automation of check processing changed the risk of misrouted and misposted checks from a discreet event associated with human, clerical error, into a systemic risk associated with the threat of malicious and accidental computer programming errors. These systemic errors resulted in entire batches of hundreds or thousands of checks being misrouted, disrupting the bank's liquidity and introducing the need, on occasion, to correct much larger numbers of misrouted checks and associated customer compensation claims.

  In addition, decisions about routing checks not only had to consider how to maximize the duration of use of customer funds but also required banks to begin to seriously consider risks associated with the counterparties to whom the checks were being routed. If the counterparty receiving the checks experienced financial or operational problems, it was possible that the bank's check settlement would be delayed. If the counterparty became financially insolvent, the delay in settlement could take months, very much impairing the bank's own liquidity. Consequently, counterparty risk management became a best practice.

  The automation of check processing was initiated and managed by the banking industry itself, in the absence of any significant regulatory guidance. It wasn't until 1987 that the U.S. Congress passed legislation to address concerns about the length of holds banks were placing on checks deposited by their customers.[4] Over the following 15 years, various regulations effectively eliminated banks' ability to exploit the use of customer funds through check routing because banks were obligated to provide funds availability to customers as quickly as the funds became available to the bank.

  Through process automation delivered by MICR technology, risk was transformed from solely being associated with low-velocity operating errors to high-velocity risk, with significant financial and regulatory ramifications.

With every opportunity digital technology has provided to banks, customers and counterparties, it has also transformed existing risk and often introduced new risk.

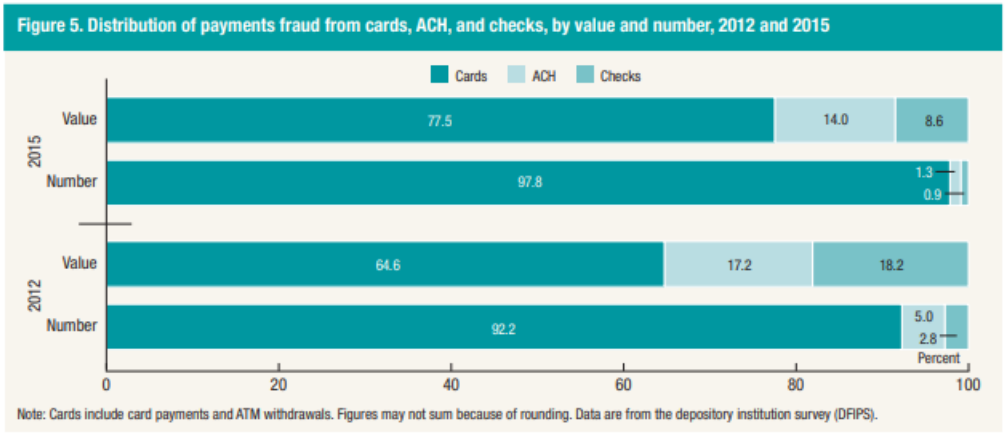
- The widespread deployment of ATMs and supporting ATM networks gave banks an opportunity to grow their customer base without significant investment in new buildings and support staff, and to retain customers at very low cost as they moved about geographically. ATMs enabled smaller banks to compete with larger banks within the same market footprint by simply expanding their ATM networks. It also allowed larger banks to penetrate smaller markets by installing an ATM in lieu of a bank branch.

  The threat of lost and stolen cash expanded from teller theft and branch robbery to the physical theft of whole ATMs, cash mishandling and theft by third parties contractually engaged to maintain the ATMs, the physical protection of customers using ATM machines, and resilience of the ATM network to ensure uninterrupted service. ATMs also introduced new, uniquely digital fraud sources such as lost and stolen ATM cards, unauthorized ATM card duplication and card skimmers, as well as raising data privacy concerns. Threat sources expanded from not only the teller or cash courier to persons stocking cash canisters, performing ATM maintenance and maintaining computer programs for when, why and how cash should be dispensed from a machine. The larger ATM networks grew, the greater the impact of an ATM network interruption on customers and on the bank's finances and reputation. Managing business resiliency risk of ATM networks became a significant concern. Lastly, existing laws such as the Americans With Disabilities Act (ADA) and Expedited Funds Availability Act (EFA) were adapted by banking regulators to apply to ATM operations. This required banks to modify physical ATMs with braille and audio assistance and to manually examine ATM deposits to place holds and provide required customer hold notifications.

- The first universal credit card, which could be used at a variety of establishments, was introduced by Diners' Club in 1950.[5] By 2012, there were almost 900 million credit cards in circulation globally.[6] This rapid consumer adoption is an indisputable indication of consumers' perception of the benefit of joining the "card economy." Like other technology developments in banking, credit cards attracted more customers to the banks that offered them. But they also gave banks a more cost-effective means for delivering credit and payment services. Banks retained traditional credit risk but introduced new and changing sources of risk primarily in the form of increased fraud and "model risk" associated with process automation.

  The Federal Reserve has estimated that "the value of fraud in total core noncash payments in the United States, estimated using depository institution survey data, rose from $6.10 billion in 2012 to $8.34 billion in 2015."[7]

By 2012, there were almost 900 million credit cards in circulation globally.



Source: Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study, Board of Governors of the Federal Reserve System, October 2018 file:///C:/Users/toburm/Documents/Solution%20Marketing/Financial%20Services/changes-in-us-payments-fraud-from-2012-to-2016-20181016.pdf

To increase banks' loan balances more quickly and cost-effectively, card-issuing banks implemented increasingly complex computer models to automate decisions regarding which consumers should be issued a credit card and how much their credit card limit should be. "Model risk" became an operational risk concern of banking regulators because poorly designed credit card models could result in banks taking on excessive future credit losses, and could introduce biases in the issuance of credit, inconsistent with the Equal Credit Opportunity Act (ECOA). Today, U.S. banking regulators pay close attention to not only model risk associated with credit issuance but also model risk associated with all kinds of models banks may use to support or supplant human decision-making.[8]

These are just a few examples of digital technology adopted by banks worldwide. The fact is that almost all banking activity today is supported by digital technology. Perhaps only for the purposes of handling physical cash do banking customers have to visit a bank building. Every other product and service offered by banks can be delivered and managed electronically. For many consumers today, money is solely digital. These consumers embody the "cashless" society.

Bank employees today (front-line, support and management) do their jobs interfacing with bank systems directly through a terminal or via a distributed network of computers. Typically, bank employees interface with systems via computers on their desktop interconnected through an elaborate telecommunication network, a part of which is invariably public-facing via the internet.

CHARACTERIZATION OF DIGITAL RISK

Digital transformation tends to change the character of existing risk and often introduces new, perhaps unexpected, risk. The following are the most common characteristics of digital risk in banking.

Dynamically Emerging Digital Risk—Digital risk arises whenever a bank introduces a new or changed product, service, business process, supporting activity or asset that is digital or relies on digital technology, including those being provided to the bank by third parties. In addition, new and expanded rules and regulations are being introduced around the world that relate to digital technology. Frequently, rules and regulations related to digital innovations do not exist at the inception of the innovation and may not emerge until years or decades later. Rules and regulations arise because of a perceived harm from the innovation itself or as a result of an unexpected outcome from the innovation.

Digital transformation tends to change the character of existing risk and often introduces new, perhaps unexpected, risk.

Greater Inherent Risk Impact—In the absence of process automation, transactions are executed and decisions are made manually, typically in a sequential fashion. Errors and fraud occurring in manual processing tend to be discrete in nature. When transaction processing is automated and errors and fraud are introduced into an automated process, the error and fraud may extend to every transaction in the process, thereby increasing the inherent risk impact should such error or fraud occur.

Increased Velocity of Risk—The onset of a material incident or loss can result much more quickly from an automated process than a manual process. Because digital risk can emerge so quickly, traditional (non-digital) means of controlling the risk are no longer effective.

Broader, More Complex Threat Sources—Process automation requires both digital technology assets and human resources with adequate technical understanding to implement and operate the technology.

- Organizations with insufficient resources to acquire, implement and maintain the technology internally often outsource the activity to third parties. While organizations can outsource the activity, they cannot altogether outsource the risk.
- Identity and access roles can be difficult to establish and maintain. For banks, unauthorized access often leads to fraud and financial loss, privacy breaches and compliance violations, financial reporting irregularities, and reputational damage.
- Technology that is publicly facing, such as via the internet, is inherently vulnerable to malicious attack. External cyber attacks have repeatedly been found difficult to detect and defend against.

- Processes that are interconnected through common technology hubs, such as a common server or telecommunication router, are vulnerable to an attack against one technology spreading to attacks against interconnected technologies. It is difficult for organizations to understand all their technology interconnections, discern the risk associated with the malicious exploitation of interconnections, and prioritize limited resources to manage the risk. It is this interconnectedness that also exposes banks to omnichannel fraud where banks must consider and manage the possibility that malicious attackers' ultimate fraud objectives are achieved by manipulating multiple communication channels—as when, for example, social engineering via telephone is coupled with online banking.
- Access to the technology user interface and to the technology itself must be restricted to authorized individuals based upon their role and responsibilities. Such restrictions must be implemented to enforce sound governance and internal control, prevent inadvertent errors, and ward off fraud and other malicious activities.

Higher-Impact Business Interruptions—The interconnectedness of banking technologies makes business interruptions more impactful to banks. The loss of power to a central processor or telecommunications hub, destruction of a centralized pool of IT assets or introduction of ransomware has the potential to bring the entire bank to a halt. The length of the interruption and cost to the bank and its customers is highly dependent upon how well the bank prepares for business interruption scenarios.

Consumer Privacy—Digital transformation in banking largely means handling consumer information. Privacy rights continue to be a focus of regulators worldwide, although many entities, including the U.S. government, have not yet passed comprehensive legislation. Banks must govern their data and manage consumer privacy risk in conformance with the Gramm-Leach-Bliley Act (GLBA) and comply with other existing, and likely to emerge, privacy regulations in the jurisdictions within which they operate.

Unknown, Emerging and Transformed Regulations—Banks that are first to innovate often find that there are few if any regulations governing their innovations. In some cases, future regulation can be reasonably anticipated. One example of regulation that can be anticipated is privacy regulation. Some privacy regulations already exist, such as the aforementioned GLBA, along with the EU General Data Protection Regulation (EU-GDPR), California Consumer Privacy Act (CCPA) and New York Stop Hacks and Improve Electronic Data Security Act (NY SHIELD). On the other hand, no regulations currently exist around the specific use of artificial intelligence (AI). Only recently have regulatory considerations about AI begun to develop.[9]

Lastly, as banks digitally transformed their business, the application of certain regulations changed as did the governance processes banks had to put into place to manage regulation. A good example of the transformation of regulations is the Bank Secrecy Act (BSA). Mechanisms to "know your customer" (KYC) at account opening changed as customers moved from physical banking to electronic banking. In addition, money movement and anti-terrorist financing concerns expanded from physical cash to electronic money movement. Today regulators are concerned about innovations such as blockchain and Bitcoin because of their complexity, how they relate to existing regulations and their impact on monetary policy.

Third-Party Risk—Many banks do not have the resources to develop and maintain their own digital products and services and support systems. In these cases, banks have turned to third parties, including cloud providers, to license the third party's offering or to have the third party provide them as a service organization. While a bank can enter into outsourcing arrangements, it cannot outsource the risk. It must understand and manage the digital risk that it is outsourcing too. This is a big consideration for EU banks subject to the Payments Services Directive (PSD).

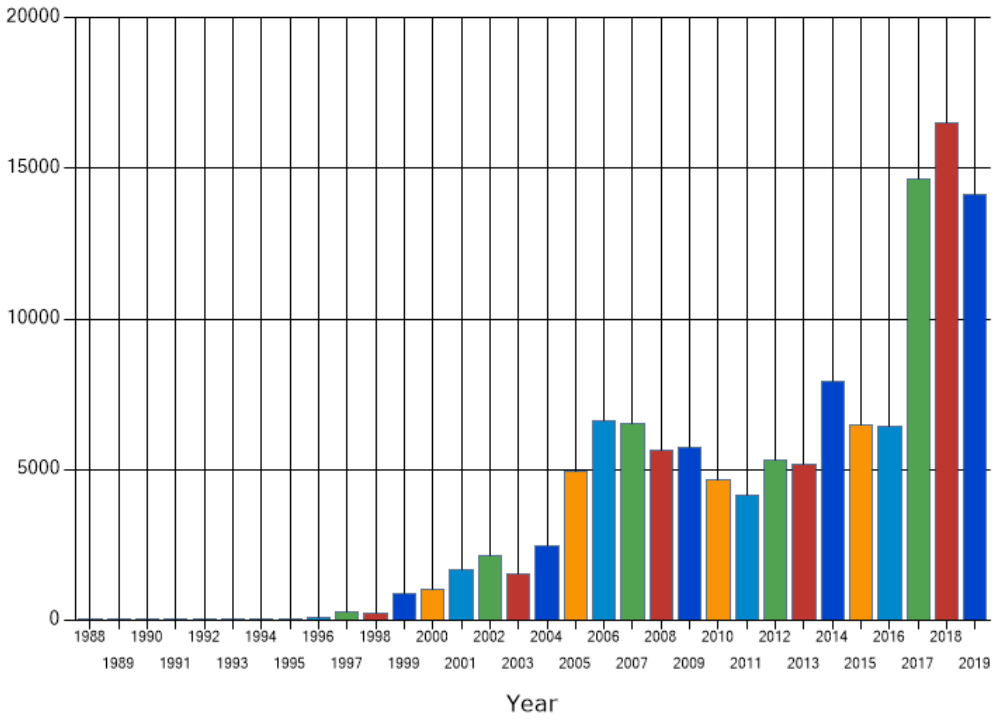
DIGITAL RISK IN BANKING TODAY

In 2019, RSA conducted a broad survey of organizations' current perception of digital risk and digital risk management priorities. The results are reported in the 2019 RSA Digital Risk Report. Eight areas of digital risk management relevant to bank survey respondents were identified, in the following order.

CYBER ATTACK RISK

Cyber attack risk was the highest risk identified by banking organizations. Banks remain concerned about cyber attacks for several reasons, including the following.

1. The volume of security vulnerabilities continues to grow.



Source: National Vulnerability Database (NVD), through 10/31/2019.

2. The financial industry continues to experience a growing number of breaches.[10]

NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	2013		2014		2015		2016		2017		2018
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1
Healthcare	176	170	242	209	239	215	301	236	305	223	256
Other Industries	152	111	138	137	176	140	116	46	59	27	159
Financial Services	80	85	87	126	154	122	145	97	156	87	134
Education	8	30	86	88	102	64	108	58	136	78	86
Professional Services	-	-	-	1	0	0	0	1	17	88	68
Government	131	65	114	180	161	138	162	127	118	89	60
Retail	56	41	82	115	132	109	122	126	147	75	55
Technology	55	57	73	67	61	63	121	84	85	59	37
Industrial	-	-	-	-	-	-	20	12	41	24	31
Hospitality	1	0	0	1	2	0	15	15	26	15	15
Insurance	-	-	-	-	1	1	9	6	11	14	15
Entertainment	-	-	-	-	3	2	20	10	37	9	11
Non-Profit	-	-	-	-	-	-	17	11	18	7	11
Social Media	-	-	-	1	1	1	1	1	6	3	6
TOTALS	659	559	822	924	1,032	855	1,163	830	1,162	798	944

Source: Breach Level Index, 2018 First Half Review, https://breachlevelindex.com

Banks intensely desire to avoid breaches, as they can result in the theft of a large number of customer records, financial damage from the theft of customer and bank assets, business interruption, and reputational damage. Breaches can trigger notification to law enforcement, banking regulators and customers. In some cases, breaches can also lead to litigation related to violations of contractual obligations around security and regulatory fines and sanctions.

3. Information technology and cybersecurity continue to be a significant supervisory priority in banks of all sizes.[11] As such, the adequacy of each bank's cybersecurity governance is subject to routine regulatory examination. Banking regulators expect management to quickly remedy any examination deficiencies identified.
4. Regulatory obligations related to cybersecurity continue to grow. Long-standing cyber-related obligations remain on the books, such as GLBA,[12] the Payment Card Industry Data Security Standard (PCI DSS)[13] and the Sarbanes-Oxley Act (SOX) as it relates to controls over the integrity of financial reporting. New cyber-related regulations impacting banks continue to come into effect, including the EU-GDPR, CCPA, NY SHIELD and New York Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies. The growth of cybersecurity regulations is expected to continue.

DATA GOVERNANCE AND PRIVACY

The second greatest concern of banks participating in the 2019 RSA Digital Risk Report is data governance and privacy. These concerns are aligned to concerns about cyber attacks. Privacy regulations and banking regulators require banks to keep customer information private, and cyber attacks often lead to privacy breaches.

The newer privacy regulations mentioned above generally have some common themes:

- Individuals "own" their information and have rights when authorizing its collection, processing and use.
- Security procedures should be implemented and maintained commensurate with the risk to individuals' privacy.
- Security breaches should be promptly reported to affected individuals.

These themes present challenges for most industries, including banking. Organizations must inventory their systems and data repositories to identify individuals' information, assess the privacy risk based on the type and amount of information being handled, and establish and maintain technical and organizational measures commensurate with the risk. They must create and maintain business processes to interact with individuals to authorize the collection and use of their information, to report how information is being used, and to notify them if and when their information is breached. These challenges cannot be addressed with a "one and done" approach. They must be addressed on an ongoing basis, including refreshing risk assessments and risk management measures when inherent risk changes or risk management best practices change.

PROCESS AUTOMATION RISK

The third greatest concern of banks participating in the 2019 RSA Digital Risk Report is process automation risk. Banks know process automation risk as an operational risk—generally, the risk of errors and fraud associated with people, processes and technology, including natural disasters. Automation risk arises whenever a new or changing product, service, activity, process or system that relies on technology is introduced or a technology-related activity is outsourced to a third party.

If the operational risks related to process automation are not carefully identified and managed, a bank may experience unexpected losses, reputational damage and potential failure. In the first section of this report we discussed three examples of process automation. In each case, risks related to the original manual business processes (check processing, cash handling, loans, deposits and payments) were transformed and new risks emerged.

To effectively manage process automation risk, banks must proactively capture business activities that may be new or changing and integrate them into the bank's risk management lifecycle. Managing this risk is considered by bank regulators as a best practice of operational risk management.[14]

DYNAMIC WORKFORCE RISK

Bank workforce dynamics continue to change, driven by employees' technology-related skills, the high demand for and short supply of workers, the use of temporary and contract labor, workers' desire for work-life balance and job flexibility, and banks' desire to maximize productivity while better managing physical plant costs.

The dynamic workforce has become an increasingly complex challenge for cybersecurity and risk management practitioners. Workforce globalization, changing demographics and rapid technology development have dramatically increased the risk associated with a progressively diverse and decentralized workforce. To effectively manage this risk, banks must be certain about who is accessing their systems, what they have access to, and what they are doing with that access.

THIRD-PARTY RISKS

There are numerous reasons banks choose to engage third parties. These include obtaining a competitive edge, leveraging vendor expertise, optimizing resources, outsourcing more cheaply than internalizing the activity, transferring risk, and capturing expanded market share in places the bank does not currently operate. When banks engage third parties to capture one or more of these benefits, they also accept risks that may arise. Risks associated with doing business with third parties include poor performance, financial risk, compliance and litigation risk, business resiliency risk, reputation risk, social responsibility risk, and strategic risk.

If banks are to manage third-party risk within acceptable levels, banks must apply robust risk management principles. This means banks must proactively identify prospective new and changing third-party relationships prior to contracts being finalized. With each new and changing third-party relationship, banks of every size must identify and evaluate the type and amount of risk the relationship poses. Only those relationships with an acceptable level of risk should be accepted.

Robust third-party risk management is not only good business practice but also an expectation of banking regulators. Failure to adequately manage third-party risk can result in one or more material risks emerging directly as a result of the relationship and from a violation of regulatory guidance.

BUSINESS RESILIENCY RISKS

The sixth greatest concern of banks participating in the 2019 RSA Digital Risk Report is business resiliency, or the ability of an organization to adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand value. It is more than business recovery; it also includes preventive and risk-driven planning, resilient measures that are built into the organization's business model, aligned security incident response and crisis management, coordinated business and IT recovery, and post-disruption strategies to reduce the impact of future disruptions.

Banking services are essential to customers, the community, and for the largest banks, the nation and the international economy. A significant interruption for any reason can have catastrophic consequences for a bank and its stakeholders. In addition, banks have compliance obligations relating to business resiliency via banking rules and regulations, and by way of contract obligations with third parties, customers and financial counterparties.

The bank's resiliency is dependent not only upon the resiliency of its internal systems but also upon the resilience of its extended ecosystem dependencies.

Where once banks worried most about business interruption from natural and man-made disasters (such as hurricanes, earthquakes, tornadoes, floods, pandemics or utility lines being accidentally cut), banks are now exposed to the significant risk of business interruption from programming errors and cyber attacks, including ransomware.

Recovery after a disruption from a cyber attack, natural disaster or man-made event is essential— but it's not enough. Many organizations must be "always on" for customers, their workforce or partners.

As a result of digital transformation, potential threat sources that could interrupt a bank's operation have expanded and become more impactful. Banks must expend more energy to identify and manage risks associated with business resiliency.

CLOUD-RELATED RISKS

Although banks have been slower to the cloud than some other industries, 46% of banks surveyed by Accenture reported they have implemented cloud-related automation, and 94% of them have a dedicated team in charge of the definition and execution of a cloud strategy, or plan to have one soon.[15]

The banking industry's interest in the cloud is the same as that of other industries: the potential to save costs, improve agility, assimilate advanced technologies and more easily integrate with technology third parties.

Banks' slow adoption of the cloud is largely related to security and risk challenges:

- **Increased access requirements**—As banks increase their adoption of cloud applications and services, more people require access to them from a variety of different devices and locations. Security teams must figure out how to provide seamless, secure access to these disparate apps that often have weak authentication policies.
- **Decreased visibility**—Security teams frequently lack visibility into their organization's complex, multi-cloud environments, which impedes their ability to proactively detect and respond to cloud-based threats.
- **Governance**—Because cloud applications and services are spread across different functions within an organization, cloud risks are not identified, assessed, evaluated, treated or monitored holistically or consistently. From the perspective of banks, cloud providers are another type of third party and must be subject to at least the same rigorous risk management standards and regulatory obligations applied to strategic third-party relationships.

COMPLIANCE RISKS

Banks view compliance broadly to incorporate three kinds of obligations: laws and regulations, the organization's own policies and procedures, and obligations created by way of customer and third-party contracts. Compliance means adherence to all these types of obligations.

There are three significant compliance challenges for banks today.

- The first and most significant challenge is simply the sheer volume of obligations. Depending on the size of the bank, the geographies in which it operates, and the type and diversity of products and services, obligations may originate from extra regional governments, individual countries' laws and regulations, state laws, industry regulators, standards organizations like NIST and ISO, practice standards organizations such as the IRS, AICP, and NEC, the bank's own internal policies and procedures, and a litany of other obligations established through contracts with customers and third parties.

  When you look at this challenge just in terms of U.S. federal regulations, during the 47 years between 1970 and 2016, U.S. federal obligations appear to have grown almost 160%.[16] Consequently, in a recent survey, the biggest challenge cited by compliance officers in 2019 was "volume and pace of regulatory change."[17]

  While banks face a mountain of obligations, and the volume of obligations is increasing, the pool of obligations is changing, too, as a result both of lawmakers and regulators changing rules and of banks expanding and transforming their strategies, the geographies within which they do business, product and service offerings, business processes, and customer and third-party relationships.
- The banking industry's cost of compliance is enormous. The Federal Reserve of St. Louis estimates compliance costs to total noninterest expense averages 10% at banks with assets of less than $100 million and 5% at banks with assets of $1 billion to $10 billion.[18] For the banking industry, Forbes estimates compliance costs totaled over $100 billion in 2016.[19]
- There are likely insufficient compliance resources to fulfill the need. The U.S. Bureau of Labor Statistics projects over the course of the next several years, the demand for compliance officers will grow at a rate of 8.2%. This is at a time when unemployment is only 2.7%.[20]

Insufficient resources, increasing program costs and ever-mounting compliance obligations mean banks cannot afford to take a check-the-box approach to compliance. They need to review their compliance programs to see if there are ways to do things more efficiently and effectively. A modern compliance program in banking today will have one or more of the following characteristics:

- Cataloging obligations to understand the scope of the compliance burden
- Establishing named accountabilities for all compliance obligations
- Using a unified control framework to map obligations to control procedures, which saves a substantial amount of time, freeing up compliance resources for more strategic work

During the 47 years between 1970 and 2016, U.S. federal obligations appear to have grown almost 160%.

- Implementing key indicators to establish continuous compliance monitoring
- Instituting risk-based compliance to prioritize the allocation of limited resources consistent with the bank's risk tolerance
- Operationalizing the capture, evaluation and management of internal and external changes that may impact the bank's compliance risk profile
- Utilizing advanced technology such as machine learning to assist in mapping new and changing obligations with control standards and risk treatments (which will also free up limited compliance resources to focus elsewhere)

A LOOK INTO THE FUTURE

Most banks continue to believe investment in digital transformation offers competitive advantage and are pursuing it as vigorously as ever for competitive reasons and financial gain. JP Morgan Chase Chairman and CEO Jamie Dimon, for example, proclaimed in his 2018 letter to shareholders that the company was "all in" for the application of artificial intelligence (AI). He listed several company-wide initiatives, including plans to deploy AI-driven robots as virtual assistants to handle tasks such as maintaining internal help desks, tracking down errors and routing inquiries.[21]

In 2015, the EU approved the revised Payment Services Directive (PSD2), in part to promote the development and use of innovative online and mobile payments.[22] Recently, as part of an effort to drive modernization of the U.S. banking system, the U.S. Treasury Department's Office of the Comptroller of the Currency (OCC) formally invited fintech companies to apply to become special-purpose national banks.[23] Both PSD2 in the EU and the emergence of fintech special-purpose banks in the U.S. are expected to impact digital risk management in banking for years to come.

HOW RSA CAN HELP

RSA Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection, and integrated risk management, RSA customers can thrive and continuously adapt to transformational change.

Integrated Risk Management—Take control of the volume, velocity and complexity of digital and non-digital risks with RSA Archer® Suite. Our best-of-breed integrated risk management solutions empower financial institutions to prioritize and manage multiple dimensions of risk using industry standards, best practices and a single, configurable, integrated software platform.

Advanced Threat Detection and Response—Increase the impact of your security team with RSA NetWitness® Platform, our industry-leading threat detection and response platform. It leverages logs, packets, endpoints and cyber threat intelligence, in addition to machine learning and security analytics technologies, to speed detection of the most advanced and elusive threats, uncover the full scope of a compromise and help automate incident response.

Identity and Access Management—Accelerate your business and minimize identity risk while delivering convenient, secure access to your extended enterprise. RSA SecurID® Suite is a comprehensive identity and access management solution that delivers capabilities for authentication, access management, risk analytics, identity governance and user lifecycle management, and it supports cloud-based and on-premises systems.

Fraud Prevention—Protect customers from data breaches, identity theft and other advanced cybercrime threats on the web and via mobile channels with the RSA Fraud & Risk Intelligence Suite. Boasting fraud detection rates up to 95%, the RSA Fraud & Risk Intelligence Suite protects more than 1.5 billion consumers around the world and has shut down more than a million cyber attacks.

RSA Risk & Cybersecurity Practice—The RSA Risk & Cybersecurity Practice offers a full set of governance, risk, compliance and cybersecurity services that include consulting, planning, implementation and cyber incident response. Our services identify and close cybersecurity, risk management and compliance gaps so that your organization can focus on core business operations and growth.

These products and services complement each other to help establish and maintain a robust digital risk management lifecycle, including addressing the risk of cyber attack, challenges of the modern workforce, cloud risk, third-party risk, modernizing compliance, data governance and privacy, automation risk and business resiliency. To learn more, please visit RSA.com.

ABOUT RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.

1 Computer History Museum, https://www.computerhistory.org/timeline/computers/

2 Bank of America revolutionizes banking industry.

3 Another Hundred Years of Cash, ATM Industry Association, Mike Lee, CEO, April 2008 https://www.atmia.com/files/ATM%20Cash%20Council/Future_of_Cash_Article_-_2.pdf

4 Expedited Funds Availability Act https://www.govinfo.gov/content/pkg/USCODE-2010-title12/pdf/USCODE-2010-title12-chap41.pdf

5 https://www.britannica.com/topic/credit-card

6 https://www.statista.com/statistics/279257/number-of-credit-cards-in-circulation-worldwide/

7 Changes in U.S. Payments Fraud from 2012 to 2016: Evidence from the Federal Reserve Payments Study October 2018, Board of Governors of the Federal Reserve System file:///C:/Users/toburm/Documents/Solution%20Marketing/Financial%20Services/changes-in-us-payments-fraud-from-2012-to-2016-20181016.pdf

8 https://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf

9 https://ai.bsa.org/wp-content/uploads/2019/09/AIHLEG_EthicsGuidelinesforTrustworthyAI-ENpdf.pdf

10 The Reality of Data Breaches, The Breach Level Index, file:///C:/Users/toburm/Downloads/breach-level-index-infographic-h1-2018-v4-22.pdf

11 Supervision and Regulation Report, Board of Governors of The Federal Reserve System, May 2019. https://www.federalreserve.gov/publications/files/201905-supervision-and-regulation-report.pdf

12 15 U.S.C. § 6801—U.S. Code

13 https://www.pcisecuritystandards.org/document_library

14 See Principle 7, Principles for the Sound Management of Operational Risk, Bank for International Settlement, June 2011. https://www.bis.org/publ/bcbs195.htm

15 Cloud and Clear, Accenture Cloud Readiness Report—Banking, October, 2018. https://www.accenture.com/_acnmedia/PDF-85/Accenture-Technology-Advisory-Cloud-Readiness-Banking.pdf#zoom=50

16 Regulatory Data on Trump's First Year, Mercatus Center, George Mason University, January 30, 2018

17 Cost of Compliance 2019: 10 Years of regulatory change, Thomson Reuters Regulatory Intelligence

18 Compliance Costs, Economies of Scale and Compliance Performance, Federal Reserve Bank of St. Louis, 2018

19 Forbes, Taming The High Costs Of Compliance With Tech, March 22, 2018

20 U.S. News & World Report. https://money.usnews.com/careers/best-jobs/compliance-officer

21 https://reports.jpmorganchase.com/investor-relations/2018/ar-ceo-letters.htm?a=1

22 https://www.fca.org.uk/firms/revised-payment-services-directive-psd2

23 https://www.reuters.com/article/us-usa-treasury-fintech/u-s-bank-regulator-allows-fintech-firms-to-seek-federal-charter-idUSKBN1KL26N