

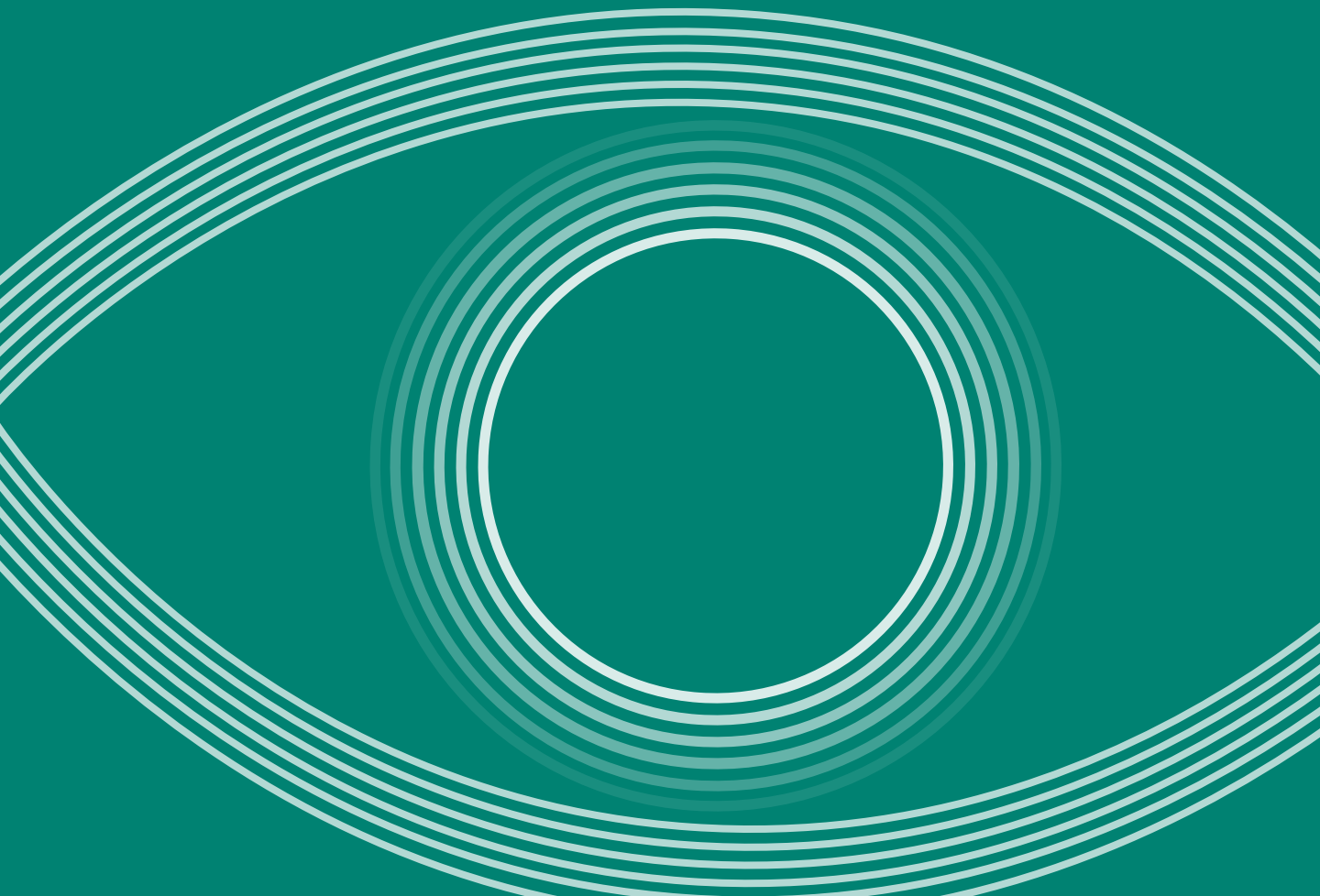
# 15



Microsoft Services

## **A new vision of cybersecurity**

Rethinking identity and access in banking and capital markets










When we think about cybersecurity, we are clearly **facing a growing problem**—a problem in need of **new solutions**.

**Brad Smith**  
President and Chief Legal Officer  
Microsoft

RSA Conference  
February 2017



# What's inside

-  03. Introduction
-  04. Built for protection
-  05. Core tensions
-  06. Crumbling defenses
-  08. In perspective
-  09. Pillars for the future
-  13. The shape of things to come
-  16. The future of design

s inside



# Introduction

FINANCIAL INSTITUTIONS HAVE ALWAYS BEEN in the trust business. But creating and maintaining trust, whether real or perceived, is no simple feat. From reinforced steel vaults to state-of-the-art digital intrusion prevention systems, banks go to great lengths to assure customers their most valued assets are safe. Like an architect designing defensible spaces in the built environment, financial institutions must put security at the forefront when drafting their business blueprints.

## Security and privacy are the foundations

Security depends on a bank's ability to verify with whom it is doing business; even an impenetrable vault cannot stop a criminal who gains access by impersonating a legitimate customer. It is no wonder banks purchase so many identity management technologies and services. Failure to properly authenticate identities can result in everything from a poor customer experience to billion dollar heists by anonymous assailants.

## Identity is the new battlefield

The concept of identity management has always been an issue for banking organizations, ranging from know-your-customer regulations to the granting of access for simple transactions. In an increasingly complex and decentralized world, the first line of defense in the battle against cybercrime is the establishment of identity—a continual challenge.

**In an era when criminal elements have access to the same resources and computing power as legitimate entities, establishing a new security model has never been more pressing for financial services organizations.**

**Security-related expenditures are growing at 8.3% compounded annually.**

Source: IDC



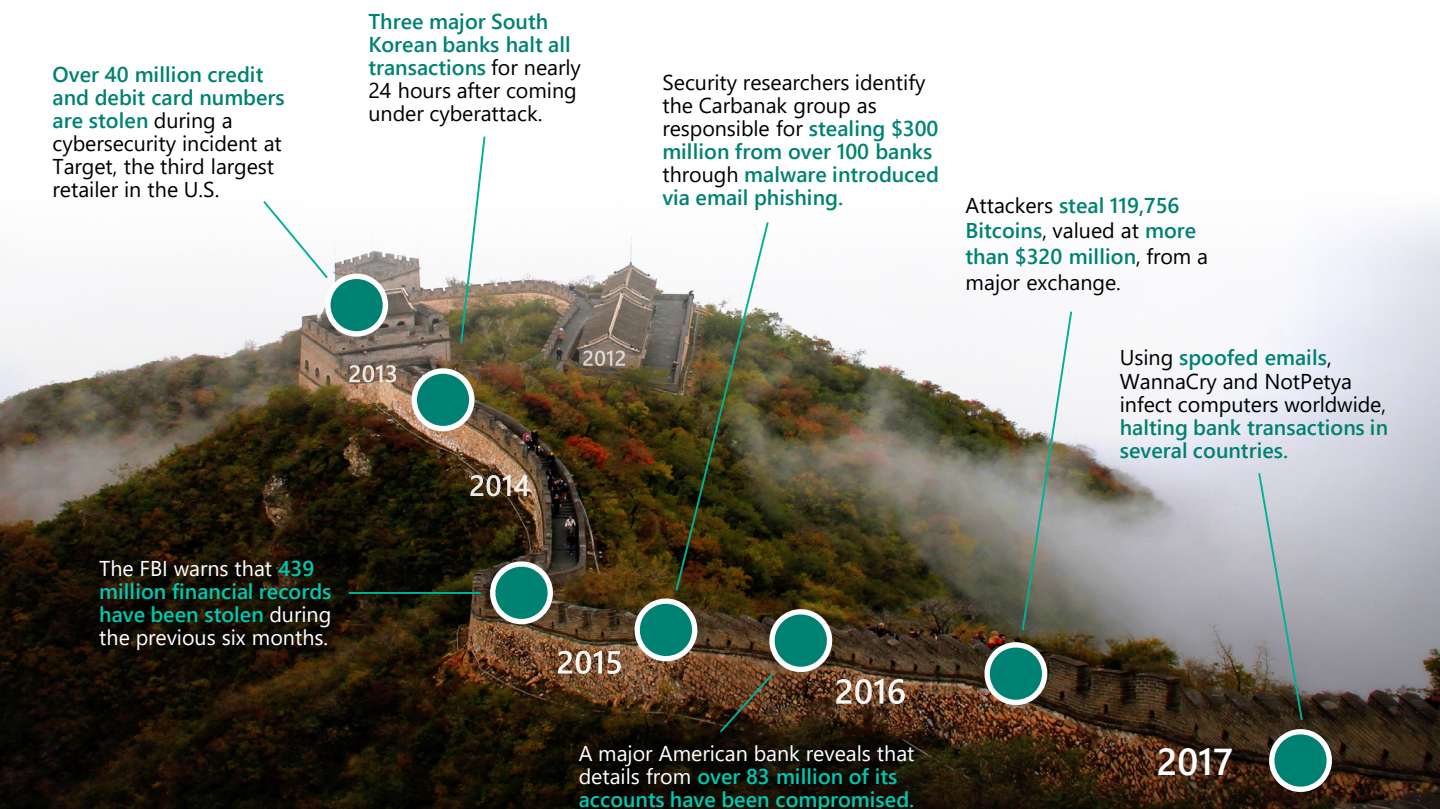


# Built for protection

FOR NEARLY ALL OF HUMAN HISTORY, the incorporation of defensive elements has been central to construction. Whether building towering guard posts or erecting walls around cities, humans instinctively seek the high ground to identify threats and defend against invaders.

In a modern context, financial institutions guard against intrusion by erecting barriers around, and restricting access to, their customers' assets. Yet, the age-old issues of theft, fraud, and money laundering are more prevalent and disruptive than ever before. The days of brazen bank robberies and getaway vehicles have given way to criminal flash mobs and digital cat burglary.

## Some notable cybersecurity incidents in the past *five* years





# Core tensions



TENSION CAN BE USEFUL in architecture. The cabling of a bridge or the keystone of an arch makes use of this fundamental force, locking constituent elements into position for weight-bearing strength and stabilizing the entire structure. In the financial services industry, however, the core tensions related to security and identity have been exceedingly difficult to balance, whether in terms of policy measures or information technology solutions—and the required investments seem never to be sufficient.

## Security and convenience

Shifting marketplace expectations regarding convenience and customer experience have further complicated security. Clients have come to expect around-the-clock global access to their finances and the ability to transact in any country and in any currency, without ever having to set foot within their financial institutions.

Balancing security with convenience has grown increasingly complex. Cybercriminals have perfected their ability to impersonate legitimate customers, while customers resist onerous security procedures. The burden of maintaining this balancing act rests on the bank: a poor experience, even for customer safeguards (such as requiring additional transaction verification) can have a lasting detrimental effect.

## Privacy and transparency

Most customers desire privacy in their personal and professional financial affairs. For financial institutions, secrecy can represent a competitive advantage: extraordinary profits will attract additional competitors and lead to loss of market share. However, such secrecy also attracts criminal elements and ultimately, intense regulatory scrutiny.

Additionally, the very nature of privacy has changed. Consumers routinely share personal information, frequently without exercising control over its use. Customers regularly express anxiety over how information about transactions, debt, and account status is aggregated, scored, and sold to third parties, often without consent.

**86% of internet users have taken steps to increase their online privacy.**

Source: Pew Research, September 2016

# Crumbling defenses

An unsustainable arms race

GIVEN THE INHERENT TENSIONS AND TRADEOFFS, the question inevitably arises: what more can banks and other financial institutions do to fend off innumerable threats, control costs, and find new ways to innovate and compete in an increasingly interconnected world? It's increasingly clear that the usual approaches to cyberdefense are simply not sustainable.

## Security expenditures keep rising

Security and identity challenges put considerable strain on financial institutions. Monetary and reputational risks along with significant regulatory pressure necessitate the maintenance of high standards.

Financial institutions spend more than \$75 billion per year on innovative security measures to deal specifically with cybercrime and privacy regulations. And, according to current data (though likely underreported due to the sensitivity of the information), security expenditures are growing at a pace more than twice other IT spending.

---

Professional **cybercriminals** will cost businesses over **\$2 trillion** by 2019.

Source: Juniper

## While criminals adapt with tech agility

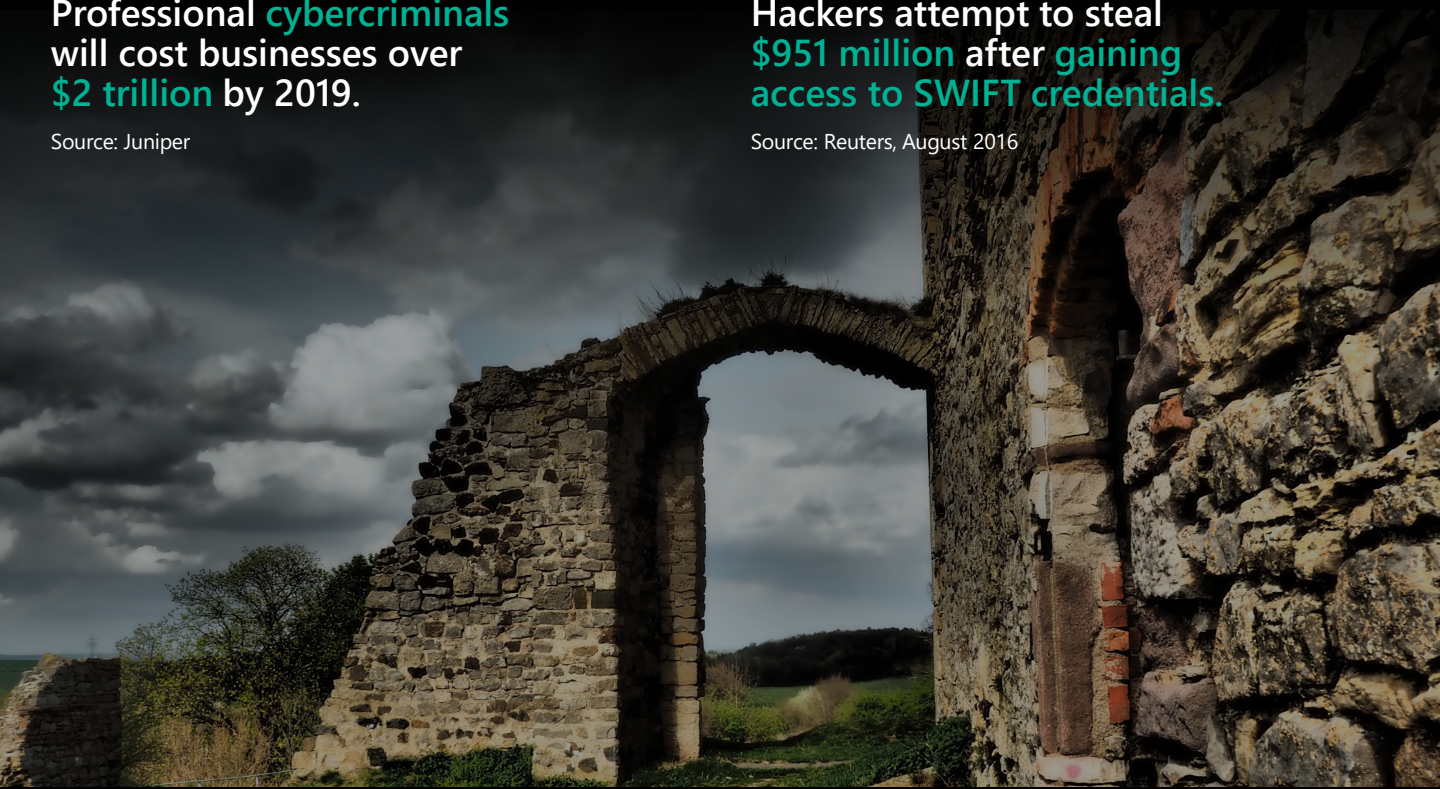
Unfortunately, criminals are also continuing to find innovative ways to circumvent cyber-defenses using technology. In the physical world, robbing a bank requires proximity to the bank vault—conditions that do not apply in cyberspace. In the digital world, billions can be stolen by an anonymous user on the other side of the planet.

It's a classic Catch-22: the solution creates the very conditions for its undoing. As a result, financial institutions are locked in a battle that cannot be won using conventional tactics.

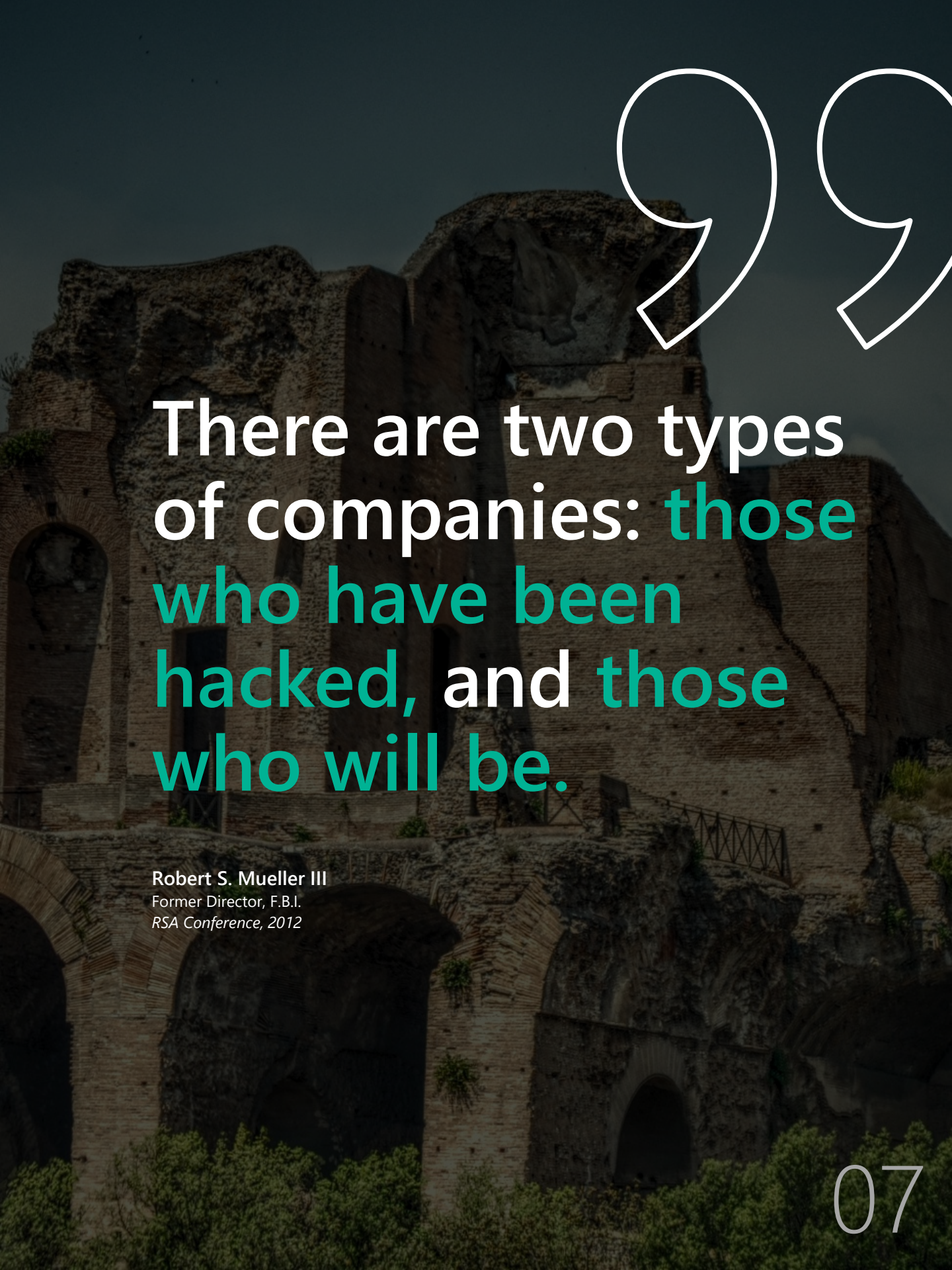
---

Hackers attempt to steal **\$951 million** after gaining access to **SWIFT** credentials.

Source: Reuters, August 2016







There are two types  
of companies: **those  
who have been  
hacked, and those  
who will be.**

Robert S. Mueller III  
Former Director, F.B.I.  
*RSA Conference, 2012*



The task is not so much to see what no one has yet seen, but to think what nobody has yet thought about that which everybody sees.

**Erwin Schrödinger**

Nobel Laureate

99

# In perspective

Reconsidering basic questions on the nature of security

BEFORE WE CAN DETERMINE A WAY FORWARD, it is useful first to take a step back, put the problem in perspective, and consider what criminals are after and how it can be safeguarded.

## What is valuable?

There are two major sources of value for financial institutions: the assets and the insights gained from data. The data itself does not create lasting value, but the information obtained through the analysis of the data with proprietary algorithms and processes does. In fact, the raw data represents a liability: it must be stored, it must be guarded, and it must meet regulatory requirements—all of which have hefty price tags.

## How can it be protected?

Financial institutions have traditionally employed technology to erect the equivalent of higher walls.

Investments in complex digital defenses and authentication procedures have done little to stem the tide of financial crimes and have only made it more difficult to respond to customer needs and market opportunities. Thus, the more defended banks are, the less responsive they become; the more defenses they erect, the more their enemies adapt. It's a vicious, and extremely costly, cycle.

## Is there such a thing as perfect security?

Perfect security is impossible. While new threats can be addressed as they arise and existing systems tested against intrusion, banks must bear an element of risk whenever financial information is accessed. As the costs mount, how much longer can financial institutions remain on the defensive?

**In sum, a new security model—a new vision—for financial services organizations is needed in the ongoing battle against cybercrime.**



A photograph of several ancient stone pillars, likely from a classical building, set against a clear blue sky. The pillars are made of large, rectangular stone blocks and show signs of weathering and age. The lighting is bright, suggesting a sunny day.

# Pillars for the future


## A new model for cybersecurity

AS GUNPOWDER AND THE INVENTION OF THE CANNON made the medieval castle obsolete, digital innovations are calling into question the current security measures at banks. Financial institutions must recognize that erecting higher walls and deploying more advanced detection systems will be losing propositions on the cyber-battlefields of tomorrow.

### Where do we go from here?

Technology innovation has also unlocked a vault of new possibilities, and we can discern the emergent principles of a new security model—a model in which financial institutions:

- I. Establish new standards for digital identity.
- II. Collaborate on defense.
- III. Reposition value and risk.



CURRENT IDENTIFICATION TECHNIQUES have been insecure for decades. Physical cards can be counterfeited and passwords can be cracked. Even biometric identifiers such as fingerprints are not perfectly secure. So how do banks control access to a trusted network when dealing with an outside party?

Traditionally, financial institutions have relied on two-factor authentication. Though not perfect, combining authentication factors is far more secure than either alone. But why stop at two or three? The main limitation is physical: identification and bank cards contain a finite amount of information, a constraint that is no longer applicable in our digital era.

### A system with memory

Imagine an authentication system that not only uses the three primary identity components—knowledge factors (e.g., password), possession factors (e.g., bank card), and inherence factors (e.g., biometrics)—but also maintains a historical record of each, generating additional context around every interaction.

### Combinatorial improvements

Leveraging technology such as biometrics and AI in combination with blockchain can provide an immutable and unique identifier. Adding a secure, cloud-based component would provide further computing power for behavior analysis, resulting in a more agile platform that reduces security risk.

### Introducing the fourth identity component

The combination of cognitive computing, predictive analytics, and the context derived from an immutable record introduces a fourth identity component—*what a person does*. The attributes of an individual's digital activity via blockchain adds even more unique possibilities and identifiers.

# Establishing a digital identity

Architecting a standard for the truly unique





Up to 95% of all AML monitoring alerts generated by a bank are false positives.

Source: PwC

# Collaborating on defense

## Forming a data ocean

THE DUPLICATIVE NATURE of legacy systems represents a major cost center and substantial security risk. A single failure could grant an intruder unfettered access to additional silos, breaching systems that were previously secure. Guarding multiple access points is less effective than guarding one, and the maintenance costs directly affect a bank's bottom line.

Market forces and pending regulations such as the EU's General Data Protection Regulation (GDPR) may be forcing the issue. By creating a single, secure, data lake to master their data, the most forward-thinking financial institutions are alleviating concerns about chain-of-custody, eliminating duplicative security measures, and reducing regulatory burdens while increasing their analytical capabilities.

## Co-opetition

The next logical step would be the creation of a secure, blockchain-powered "data ocean" by a bank consortium.

Raw data is a risk from both a security and a regulatory perspective, and the data has little value on its own. With a secure, cloud-based blockchain, individual banks would no longer have to create and maintain their own data warehouses. Banks could eliminate data redundancy and share the cost of storage.

## Precedent

Though the concept of data sharing may seem foreign to many banks, the model for it already exists within financial institutions and has been employed for many decades in capital markets. Market data is widely disseminated; market participants compete and offer value-added services with trading strategies, custodial services, and account advisory.

Imagine if customer data were treated in the same manner: the aggregate data would reside on a secure platform, each member bank would improve its customer understanding, and members could focus on delivering enhanced solutions derived from deeper information.

# Repositioning value and risk

Empowering customers and reducing criminal incentives

WHAT IF BOTH THE RAW DATA and a customer's account value resided outside the confines of a financial institution? In practice, only a small percentage of money on deposit is in the bank at a rate determined by the reserve requirements. The bank's true value lies in its ability to connect those who have capital with those who need it—as Airbnb or Uber are connecting supply with demand.

Though regulations will take time to catch up with innovations, in a decentralized and digital world where value can be moved around in real-time, *does the location of the funds matter?*

## The nature of deposits

Imagine a future in which a customer possesses her raw financial data and

account balance, secure in a personal cloud or digital wallet, and linked to her digital identity. Financial institutions would market their trusted status and banking relationships to gain access to customer funds, not as deposits, but as revolving short-term credit—a personal version of commercial paper.

Banks would act as pass-through vehicles, as trusted connectors, or as clearinghouses—collecting net interest spread as compensation for bearing the risk of contract guarantees.

## Economic viability of crime

Lacking large targets and central stores of value, financial institutions would be less likely to incur the unwelcome attentions of

cybercriminals. Despite the massive increase in potential targets, the payoff for gaining access to the average account would be minimal. The scanty proceeds received from hacking a single account would not be worth the effort.

As a result, digital theft would become less economically attractive and money laundering would become far less appealing. It would be increasingly difficult to hide ill-gotten gains in aggregated stores of value once value was widely disseminated. Creating complex and confusing transactions to camouflage illegal money sources (a process known as layering) would become less common as financial institutions began to employ an immutable financial record shared among member banks that tracked customer funds.

---

Why do I rob banks?  
Because that's where  
the money is.

Willie Sutton





A low-angle, upward-looking photograph of several modern skyscrapers with glass facades, creating a sense of height and architectural scale. The buildings are arranged in a way that they seem to converge towards the top of the frame.

# The shape of things to come

IT HAS BEEN OVER TWO MILLENNIA since Vitruvius wrote *De Architectura*, describing the three pillars of architecture—usefulness, strength, and beauty—and the notions of proportion that serve as the classical basis for architectural thought.

## Building opportunity

The three modern pillars of security—digital identity, collaboration across business boundaries, and decentralization—can dramatically shift how financial institutions address cybercrime and frame future business opportunities. Consider the possible shape of a future built on these pillars, in which banks empower a dynamic new matrix of financial privacy, security, and trust.





# Reconstructed privacy

## *Data mastery, revisited*

The combination of digital identities and decentralization promises to change how banks handle privacy concerns and has implications far beyond the financial world. Customers become the masters of their own data, selectively granting access—whether in whole or in part, persistently or temporarily—to different aspects of their digital identities and financial information.

Powered by advanced analytics and AI, financial institutions become the vanguards of privacy, empowering their clients with more control over their data. In this vision, banks become trust and identity brokers, providing customers with on-demand services and acting as secure access points to the data oceans.





# Spanned structures

## Trusted intermediaries

In a perfectly trusted network, all participating individuals and institutions—*all nodes*—are known entities. In this context, financial institutions will be uniquely positioned to catalyze, and serve as essential intermediaries in, interdependent banking networks.

Imagine banks as the arbiters of trust, employing [augmented intelligence](#) capabilities and blockchain solutions to safeguard customer data and assets, and serving as the bridge that consumers and institutions use when conducting business in a digital world. Some services will be centralized and closely controlled, offered only to trusted partners via APIs; others will be distributed across business boundaries in discrete, embedded applications that bear the bank's imprimatur.

## New business opportunities

Unburdened by legacy costs, financial institutions will become highly secure and agile platforms that offer tailored products, value-added services, and secure infrastructure, focused on monetizing customer relationships, unique data insights, and new business opportunities.

High-revenue activities, such as extending credit, financial advisory, and capital market services would still be available, but now with much lower overhead. Other opportunities, ranging from as-a-service offerings to plug-and-play analytical services, will give financial institutions the ability to connect clients with other entities and explore new lines of business—solidifying the role of banks at both the center and the edges of a [new banking ecosystem](#).



# The future of design

IN ARCHITECTURE, a better understanding of material properties and the ability to create complex and precise models have enabled engineers to create unique buildings that were once considered impossible, pushing design towards a second Renaissance.

Financial institutions are also on the verge of a rebirth. In a digital economy, financial institutions must architect for agility and new business models; embedding technology directly into products and services is changing how financial services deliver value.

At Microsoft, we understand security is the cornerstone for financial institutions—we've invested billions of dollars in creating secure, enterprise-ready technologies that enable our enterprise customers to adapt and compete in a rapidly changing marketplace. And our cybersecurity architects help them transform their critical attack defenses, reducing vulnerabilities and improving their ability to detect and respond quickly to emergent threats.

**Our approach applies technology in unique ways—with a trusted cloud platform, tools, and services that empower business agility and enable the future of banking.**

**We are at the forefront of predictive analytics and cognitive services.** At Microsoft, we're focused on building AI solutions that span infrastructure, services, apps, and agents—arming financial institutions with the agility and innovation they need for the battle against cybercrime.

**We understand the complexities of biometrics.** Our comprehensive approach to IoT and biometrics helps our customers secure identities, data, and infrastructure, all while enabling a more flexible and convenient experience.

**We provide financial services-ready cloud solutions to help banks create an open, agile, and secure platform.** Underpinned by productivity, collaboration, and unified communication tools, Microsoft enables widely distributed and highly regulated financial institutions to build the environment needed to function as agile, innovative organizations.

**We are innovative digital advisors on blockchain architecture.** Backed by a cloud platform with the largest compliance portfolio in the industry, our Blockchain-as-a-Service provides a rapid, low-cost, low-risk, fail-fast platform to enable financial institutions to collaborate.

# What's next?

No matter where you are on your digital transformation roadmap, Microsoft can help.



## Engage your customers

Reimagine the client experience for a digital world and deliver more value through insights and relevant offers by engaging clients in natural, highly-personal, and innovative ways throughout the customer journey—driving increased relevance, loyalty, and profitability.



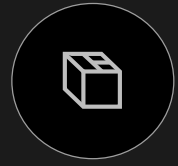
## Empower your employees

Empower a high-quality and committed digital workforce to work and collaborate as a team anywhere on any device with modern productivity tools that provide seamless access to your data—helping you innovate faster, meet compliance requirements, and deliver exceptional client experiences.



## Optimize your operations

Gain breakthrough insight into risk and operational models with advanced analytics solutions and act on real-time intelligence to optimize risk management and meet regulatory requirements.



## Transform your products

Drive agility with open and connected systems and highly-automated digital processes to support new product development and optimize distribution channel strategies while meeting the security, privacy, and transparency expectations of customers, regulators, and shareholders.

Contact us today for more information.

# What's next?



**Kenneth Parker**

Managing Director  
Worldwide Banking & Capital Markets



**Juliet Gritz**

Financial Services Lead  
Worldwide Industry



**Carr Phillips**

Product Marketing Director  
Worldwide Financial Services



MANY SUBJECT MATTER EXPERTS from various groups around Microsoft contributed to the concept and articulation of the story contained in this document. Above all, we wish to thank **Kenneth Parker**, **Juliet Gritz**, and **Carr Phillips** for their sponsorship in its creation.

- **Dave Morehouse**, Sr. Worldwide Marketing Manager for Microsoft Services
- **Andrew Longstaff**, Sr. Audience Marketing Manager, Worldwide Industry

## Contributors

**Britt Boston**, Security Solutions Manager  
**Tim Bowman**, Information Alchemist  
**Andre Burrell**, Sr. Industry Solutions Manager  
**Steve Butcher**, Sr. Industry Architect  
**Alma Cardenas**, Sr. Business Program Manager  
**David Cox**, Executive Director, Microsoft Digital  
**Danelle Darroch-Conners**, Editorial Consultant  
**Victor Dossey**, Industry Strategy Director  
**Peter Hazou**, Business Development Director

**Chris Jackson**, Sr. Cybersecurity Architect  
**Darren Jefford**, Industry Architect  
**Aman Kohli**, Chief Architect  
**Steve Leigh**, Business Development Director  
**Daragh Morrissey**, Sr. Industry Technology Strategist  
**Rupert Nicolay**, Architect  
**Dan Palmer**, Strategy Philosopher  
**Binil Arvind Pillai**, Security & Identity Solutions Director  
**Berk Veral**, Sr. Manager Cybersecurity



Microsoft Services empowers organizations to accelerate the value imagined and realized from their digital experiences.

Imagine.  
Realize.  
Experience.

[microsoft.com/services](https://microsoft.com/services)

