

Cyber Fears in Financial Services




**6 Cybersecurity Trends, Challenges, and Common
Misconceptions Plaguing the Financial Services Industry**

Introduction

It's been a busy few years for the financial services industry, as a wealth of new digital products and services are changing how customers interact with their money. But the added network complexity that these tools deliver is making financial networks more distributed and harder to defend, and hackers are finding new and surprising ways to exploit holes in security to breach sensitive data.

In this eBook, we take a look at some of the more eye-opening trends taking place in the realm of cybersecurity, specifically where it pertains to the financial services sector.

- 
- 1. Compliance is Only a Starting Point for Finance**
 - 2. Insiders Cause the Majority of Data Breaches**
 - 3. The Cleaning Crew Could be a Hacker's Ticket In**
 - 4. Increased Reach—Not Sophistication—is Fueling Most Breaches**
 - 5. Just Like Threats, Solutions are Constantly Evolving**
 - 6. Your Son or Daughter Could Be Next Big Cybercriminal**

[CONTINUE READING](#) ►

Compliance is Only a Starting Point for Finance

Complying to regulation is a good starting point for mapping out a cybersecurity strategy. But allocating an entire security budget toward meeting the latest standards from NAIC, CFTC and NYDFS, for instance, can create a defense that focuses too much on regulation and not enough on evolving threats.

Financial services organizations need to balance their security budgets to embrace new technologies that do more than just the bare minimum. Because a customer's trust is the most prized asset for any financial institution, budgets need to leave room for the adoption of new technologies that can address threats as they come to the fore.

For large banks (\$1 billion to \$10 billion in assets) total compliance costs an average of \$1.8 million, or 2.9% of their noninterest expenses¹



¹ Scale Matters: Community Banks and Compliance Costs

Insiders Cause the Majority of Data Breaches

In cybersecurity and in horror movies, sometimes the scariest threats come from “inside the house.” For banks, employees at any level can very easily, whether inadvertently or maliciously, be exploited by thieves looking to access network data. In finance, in particular, the darknet is chock full of marketplaces where access to a bank’s network can reap a high price tag, enticing less-than-loyal employees to turn on their bosses and customers.

A 2015 insider data breach at Morgan Stanley exposed more than 700,000 accounts²

2 Guilty Plea in Morgan Stanley Insider Breach

The most efficient way for companies to detect this threat is to have insight to activity taking place within the network, not just filters for traffic entering or exiting. Application use, for instance, should be monitored to flag for programs that may appear innocent but are actually usurping sensitive company data.

Among 874 incidents, as reported by companies to the Ponemon Institute for its recent **2016 Cost**

of Data Breach Study, 568 were caused by employee or contractor negligence; 85 by outsiders using stolen credentials; and 191 by employees and criminals.

65% of breaches
were caused by insider negligence

The Cleaning Crew Could Be a Hacker's Ticket in

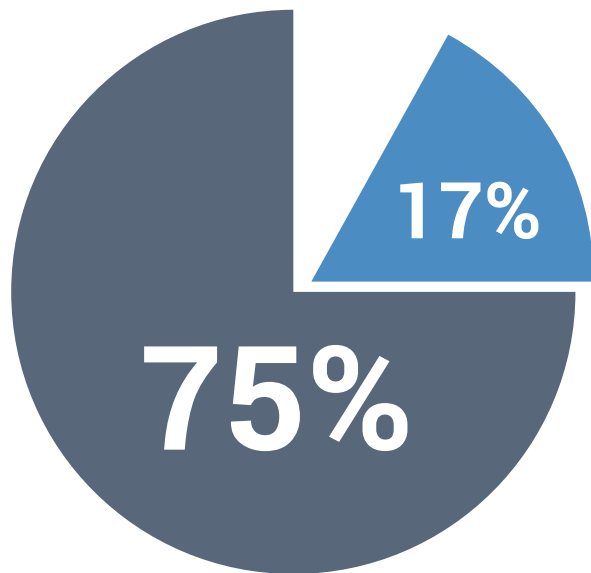
It's intuitive that hackers will exploit the easy points of access to the network to commit their crimes. Financial services businesses may think they're implementing so much network and endpoint security that there simply aren't any easy points of access to sensitive data for hackers to exploit. But what about the third-party contractors or service providers these organizations employ?



Maintenance companies and office suppliers, for instance, may not have nearly as many security protocols in place as a bank, but they certainly can email an institution's billing or operations departments. Phishing scams can infiltrate the bank network by hiding behind familiar third-party email addresses that billing and ops wouldn't hesitate to open, unleashing malware onto the network that can steal PII or even drain accounts. Banks need to ensure that they aren't just filtering URLs, but also taking a microscope to the files that come over the network by beefing up their gateway solutions.

Increased Reach – *Not Sophistication* – is Fueling Most Breaches

While one may assume that malware threats are getting more sophisticated with time, it's really delivery methods that are evolving quickest, not necessarily the programs themselves. By using phishing schemes or social engineering, malicious actors have been able to leverage greater reach to successfully infect financial networks on a massive scale.

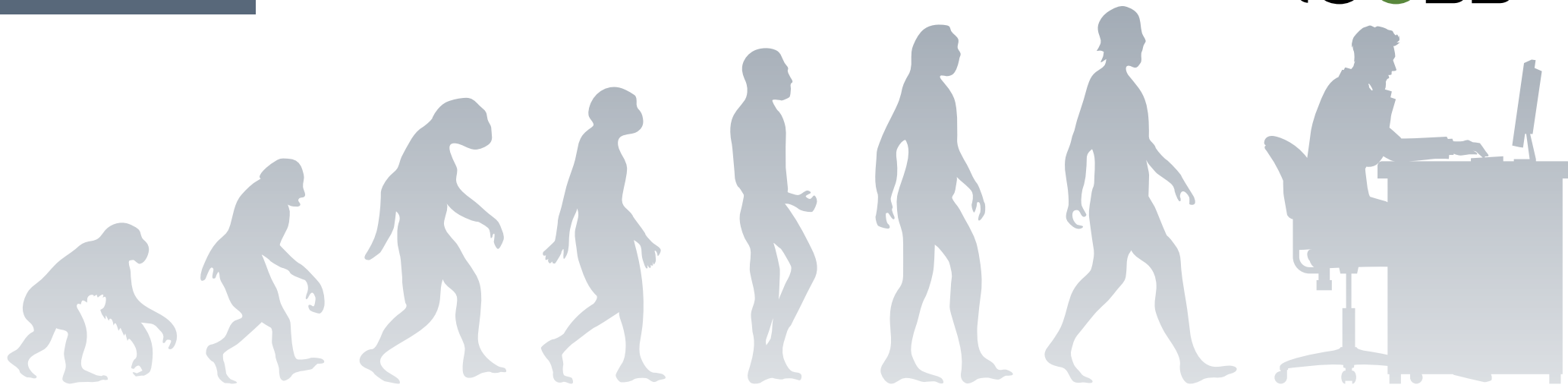


Social Engineering vs. **Sophisticated Malware**

Social Engineering Outshines Sophisticated Malware

Although more technical and sophisticated software is harder to crack—and has a higher success rate than many of the more common malware programs out there—nearly three quarters of all fraudulent incidents reported last year by a leading bank to [cybersecurity group Kaspersky Labs](#) were a result of social engineering. On the other hand, sophisticated malware only accounted for 17 percent.





Just Like Threats, Solutions are Constantly Evolving

Financial services organizations can't simply install a comprehensive security architecture and call it a day, leaving the protocols and proxies in place until they fail, and only then modifying as they see fit. This is irresponsible and costly, since recuperating from a data breach is usually far more expensive than continually testing and improving network defenses.

Data breaches now, on average, cost banks \$4 million per incident³

3 Fortune: Data Breach Cost Study

Sophisticated detection tools that go beyond standard web filtering are therefore a must, with technologies like penetration testing and file sandboxing, which allows suspicious files to play out in a simulated network environment to determine if they are unknown malware, can help beef up the network on an ongoing basis.

Your Son or Daughter Could Be Next Big Cybercriminal

An emotionally distressing aspect of cybercrime is that those committing it are getting younger, on average. Malware-as-a-service has emerged, putting prebuilt programs in the hands of individuals looking to make a quick buck, who are increasingly young, tech-literate hackers who grew up with the internet. Because these individuals grew up in an environment where cybercrime was relatively common, they're less deterred by the impulse to pursue aggressive crimes, like unleashing bank malware, than those in generations before them.

While there isn't much financial businesses can do to change the mindset of an entire generation, understanding the mindset of today's hackers drives the point home that financial services need to be adamant in enforcing a layered defense. Accessing malware has never been easier, and this presents an easy pay day for individuals who have been hackers since childhood.

**In the span of just 12 months
(2014 to 2015), the average
age of cybercrime suspects
dropped from 24 to 17⁴**

⁴ Average Age of Cyber Attack Suspect Drops to 17





The Biggest Takeaway...

The biggest takeaway for IT teams tasked with managing cybersecurity for financial networks is that the job is never done. Malicious actors will always be coming out of the woodwork, employing new and sometimes unexpected tactics to access funds and PII. IT teams therefore have to not only be vigilant, but keep the big picture in mind when mapping out their constantly-evolving network defenses by planning for tomorrow's threats today.

About iboss

The iboss Distributed Gateway Platform is a web gateway as a service that is specifically designed to solve the challenges of securing distributed organizations. Built for the cloud, iboss leverages a revolutionary, node-based architecture that easily scales to meet ever-increasing bandwidth needs and is managed through a single interface. The iboss Distributed Gateway Platform is backed by more than 110 patents and protects over 4,000 organizations worldwide, making iboss one of the fastest growing cybersecurity companies in the world.

To learn more, visit www.iboss.com or contact iboss at sales@iboss.com