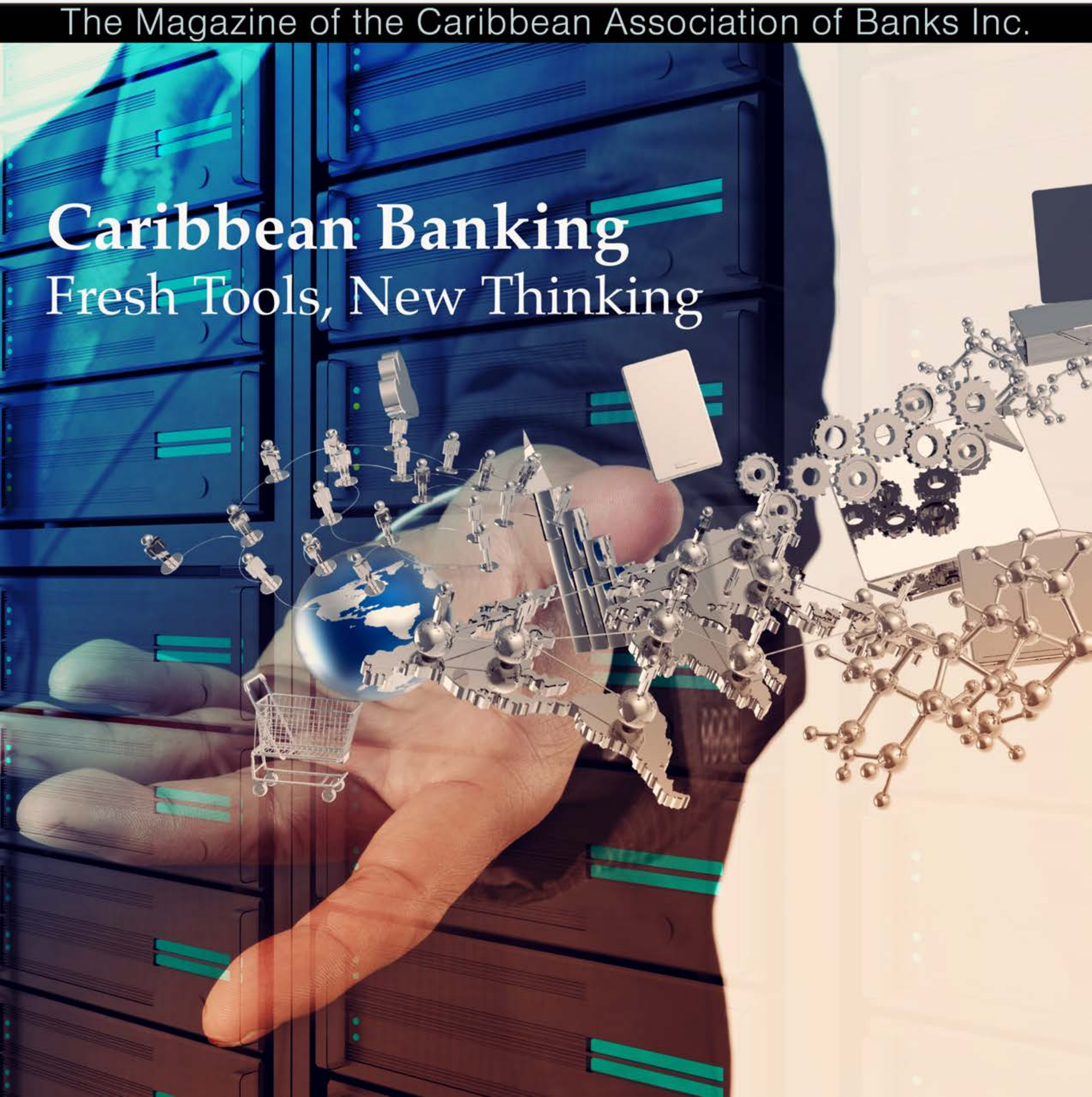
CAB CARIBBEAN account 2016

The Magazine of the Caribbean Association of Banks Inc.



Caribbean Banking
Fresh Tools, New Thinking

Caribbean Association of Banks Inc.

Vision

Caribbean Association of Banks Inc. will be the focal point for networking and effective advocacy, and the organisation of choice for support and services for financial institutions in the Caribbean region.

Mission

To advance the interest of member institutions through advocacy, networking, provision of training and other solutions to strengthen the Caribbean financial services sector.

Value Proposition

- Superior Advocate
- Premier Networking Platform
- Best Information Source
- Responsive, Efficient, Effective Service Delivery

Core Values

CAB members, Board and staff will be guided by the following.

- Integrity: We are truthful and transparent, and deliver what is promised.
- Commitment: We agree to live up to our responsibilities and operate in keeping with the highest international standards.
- Confidentiality: We adhere to agreements and standards on disclosure of information.
- Cooperation: We are willing to work with others to achieve a common goal.
- Accountability: We accept responsibility for our actions.

Core Objectives

- To foster a spirit of goodwill and camaraderie among the Banks and Financial Institutions of the region with a view to solving their common problems through understanding and co-operation.
- To assist in and influence the development and improvement of the codes of conduct and standards of the Banking and Financial Services Industry in the Caribbean/ CARICOM Region.
- To provide a forum for the exchange of ideas and information on various aspects of operations in order to broaden the scope and knowledge of its officers.
- To assist its members wherever possible in the areas of training, management, systems and processes, inspection or any other related areas of operations.
- To collect and disseminate statistical, technical, economic and other information relating to banking and all its aspects.
- To print and publish any magazines, newsletters, periodicals, books or leaflets that the Association may consider desirable for the promotion of its objectives.
- To foster an increasing awareness of the presence of its members at the Governmental level and to seek assistance in promoting its objectives.
- To do whatever is deemed necessary within the limits of its members' powers to develop and strengthen Banks and Financial Institutions of the Caribbean/CARICOM Region.
- To amalgamate with any companies, institutions, societies or associations having objectives altogether or in part similar to those of this Association.

The Caribbean Cybersecurity Landscape: What Financial Institutions Need to Know

Revolutionised by the digital era, banks today are more vulnerable than ever to cyber threats. While there have been no recorded events of data theft in the Caribbean, there is plenty of evidence that organisations of all shapes and sizes have been infiltrated at some level. "With over 50 financial institutions in the Caribbean, it is only a matter of time until the first data breach occurs," says the author, in this article, which presents ten effective security habits to protect the financial institution.

Today's cyber security threat landscape is becoming increasingly complex, and more and more organisations are falling prey to cybercrime. With data theft on the rise globally, hardly a day goes by without another headline about how disruptive technologies place information at risk for data leakage, credit card fraud, hacking and other security breaches.

It goes without saying that organisations processing or storing the largest amounts of critical data, such as financial institutions and governmental entities, are the targets and consequently often the biggest victims of data theft. Examples include the Central Bank of Bangladesh with a theft of US$81 million, the First Bank Taiwan with an ATM malware heist of US$2 million, the loss of account information at JP Morgan Chase affecting 76 million households and seven million small businesses, and the leaking of thousands of client data for Invest Bank in the United Arab Emirates by a hacker who threatened to leak the information unless he was paid US$3 million.

> "The modern thief can steal more with a computer than with a gun[1]"

New Vulnerabilities: The banking industry has been revolutionised by the digital era. Banks have become global financial virtual super stores; offering online banking services that are available 24 hours a day, 365 days a year. This level of electronic customer access makes banks more vulnerable to cyber threats and consequently forces them to find effective solutions to protect their financial assets. Cybercrime is becoming an important issue not only for CIOs and IT professionals, but also for CEOs, CFOs, compliance officers, boards of directors, and business owners. The questions remain the same: "Is the Caribbean a safe haven or is my financial institution at risk? And if so, how can I protect my critical data assets from cybercrime?"

The Caribbean – A Safe Haven? According to a recent study from the Ponemon Institute, "the average total cost of a data breach increased from $3.79 million to $4 million"[2] worldwide from 2015 to 2016. While there have been no recorded events of data theft in the Caribbean, there is plenty of evidence that organisations of all shapes and sizes have been infiltrated at some level. In fact, heavily regulated industries such as the banking industry generally experience the most costly data breaches due to "higher than average rate of lost business and customers"[3] and fines. With more than 50 financial institutions in the Caribbean, it is only a matter of time until the first data breach occurs. Research suggests that the Mean Time to Identify (MTTI) a breach is 201 days with an added Mean Time to Contain (MTTC) of 70 days (for a total of 271 days)[4]. The longer it takes to detect a breach, the costlier it becomes because hackers have more time to locate and exfiltrate data. It is therefore plausible to assume that several banks may already have been hacked or are being hacked without knowing it. Caribbean banking customers have every right to question how secure their financial assets really are.

In addition, the Caribbean financial services industry has recently been hit by the so-called "de-risking" movement. Over the past four years, US financial institutions have tightened their regulatory noose and ended relationships with certain Caribbean banks to protect themselves from financial fraud, money laundering and terror financing. This de-risking or "de-banking" movement threatens the Caribbean banking industry and fosters isolation amongst the global financial community. According to Reuters Investigates (2016), "the loss of banking ties to the U.S. endangers the region's economic stability by inhibiting trade, banking and government officials say"[5]. Now more than ever, Caribbean financial institutions have a reason to protect their corporate brand and image and secure their most valuable asset – their data.

> "There are no quick fixes, no magical solutions to prevent cyberattacks not even in the Caribbean, a region known to be 'secure' "

Along with pressure from their banking customers and tighter scrutiny by US federal regulators for the sake of de-risking, Caribbean financial institutions are also under great scrutiny from the United States to meet strict compliance requirements. Enacted in 2010, the Foreign Account Tax Compliance Act (FATCA) "requires foreign financial institutions (FFIs) to report to the US Internal Revenue Service (IRS) information about financial accounts held by US taxpayers, or by foreign entities in which US taxpayers hold a substantial ownership interest"[6]. As of August 30, 2016, nine Caribbean countries are under FATCA compliance: Bahamas, Cayman Islands, St. Kitts and Nevis, Barbados, Curaçao, St. Vincent and the Grenadines, British Virgin Islands, Jamaica and Turks and Caicos Islands. Caribbean governments have been under pressure to sign the relevant agreements, and failure to comply often results in stiff penalties inclusive of losing their correspondent banking relationships for the domestic banks.

Most recently, the Caribbean Association of Banks (CAB) itself encouraged all Caribbean countries to comply with FATCA by signing Intergovernmental Agreements (IGAs) before December 31, 2016[7]. To avoid hefty fines and comply with regulations, Caribbean financial institutions are best advised to form a corporate compliance committee, or at minimum appoint a Compliance Officer to manage compliance before and after becoming FATCA compliant. Unfortunately, many financial institutions do not have the necessary funds or internal expertise to do so. A trustworthy security service provider can assist in implementing and maintaining an organisation-wide compliance program.

10 Effective Security Habits to Protect your Financial Institution: We've gathered the most effective security best practices you can implement to better secure your critical data assets and improve your security posture.

1. Focus on the right threats

The average company faces threats from malware, human adversaries, corporate hackers, hacktivists, governments and even malicious insiders. In order to be truly secure, we are asked to install hundreds of patches each year to operating systems, applications, hardware, firmware, computers, tablets, mobile devices, and phones – yet zero day exploits and other security issues leave us vulnerable. Take the time to identify your company's top threats, rank those threats, and concentrate the bulk of your efforts on the threats at the top of the list.

2. Know what you have

Establish an extensive, accurate inventory of your organisation's systems, software, data, and devices. Most companies don't have a comprehensive understanding as to what is really running in their environments. How can you even begin to secure what you don't know? The best companies have strict control over where their critical assets are in the organisation.

3. Remove, then secure

An unneeded program is an unneeded risk. The most secure companies pore over their IT inventory, removing what they don't need, then reduce the risk of what remains. This applies not only to every bit of software and hardware, but also to their data as well. Eliminate unneeded data first, then secure the rest. Intentional deletion is the strongest data security strategy. Make every new data collector define how long their data needs to be kept. Put an expiration date on it. When the time comes, check with the owner to see whether it can be deleted.

4. Run the latest versions and patch quickly!

This advice is so common it has become a cliché: Patch all critical vulnerabilities within a week of the vendor's patch release. If your company takes longer than a week to patch, it's at increased risk of compromise – not only because you've left the door open, but because your most secure competitors will have already locked theirs. Also, the best security shops stay up on the latest versions of hardware and software. The latest software and hardware comes with the latest security features built-in, often turned on by default. The biggest threat to the last version was most likely fixed for the current version, leaving older versions that much juicier for hackers looking to make use of known exploits.

5. Educate your users!

Education is paramount. Unfortunately, most companies view user education as a great place to cut costs, or if they educate, their training is woefully out of date, filled with scenarios that no longer apply or are focused on rare attacks. Effective user education focuses on the threats the company is currently facing or is most likely to face. It should be led by professionals and must involve the employees themselves. Security staff also needs up-to-date security training each year to stay informed about the latest threats to corporate security.

6. Keep the configurations consistent

The most secure organisations have consistent configurations with little deviation between computers performing the same role. Most hackers are more persistent than smart. They simply probe systems and applications, looking for that single vulnerability in thousands of servers that you forgot to fix. By implementing consistent change management, you can establish configuration baselines and rigorous change and configuration control. Admins and users should be taught that nothing gets installed or reconfigured without prior documented approval. Find the right mix of control and flexibility to avoid committee paralysis. At the end of the day, make sure any change, once ratified, is consistent across computers.

7. Use least-privilege access control

"Least privilege" is a security maxim which means giving the bare minimum permissions to those who need them to do an essential task. Most security domains and access control lists are full of overly open permissions and very little auditing. The most secure companies have automated processes that ask the resource's owner to re-verify permissions and access rights on a periodic basis.

8. Institute smart monitoring practices and timely response

The vast majority of hacking is actually captured on event logs that no one looks at until after the fact, if ever. The most secure companies monitor aggressively and pervasively for specific anomalies, setting up alerts and responding to them. Good monitoring environments don't generate too many alerts. In most environments, event logging, when enabled, generates hundreds of thousands to billions of events a day. Certainly not every event is an alert, but an improperly defined environment with rules that are not optimised will generate thousands of potential alerts – so many that they end up becoming noise that everyone ignores. Some of the biggest hacks of the past few years involved ignored alerts, the sign of a poorly designed monitoring environment. The most secure companies create a comparison matrix of all the logging sources they have and what they alert on, then compare this matrix to their threat list. Then they tweak their event logging to close as many gaps as possible. More important, when an alert is generated, they know it is significant and they respond.

9. Create an Incident Response Plan

No organisation is immune to data breaches, and financial institutions especially will remain targets for cybercriminals. When a breach happens, what are you going to do? Do you have a strategy in place to deal with the impact of a breach? What will be your priorities and next steps? And how will you communicate the news to your staff and customers? An incident response plan is the most important measure of today's data security best practices but is sadly overlooked by most organisations. Get all relevant departments involved to agree on what to do following a data breach, and an incident response plan will help you get through the aftermath of a data breach without panicking or making aggravating mistakes. Once created, the plan needs to be rehearsed and an incident needs to be simulated to cover all possible scenarios, gain habits and establish mechanisms for emergencies.

10. Seek help from a trusted and reputable security provider

No one performs heart surgery on themselves or attempts to remove an aneurysm at the dining table. This is something that is left up to the experts. In the same manner, companies should recognise their core competencies and leverage trusted and reputable partner experts to assist them with their security issues. This is an area where almost all companies are the weakest!

In conclusion, the decision to buy, implement and maintain solutions against cybercrime can be quite challenging and those responsible are often overwhelmed with the sheer variety of security solutions. Although there are hundreds of ways to become marginally more secure, there are no quick fixes, no magical solutions to prevent cyberattacks – not even in the Caribbean, a region known to be 'secure'. Regardless of the size of your organisation, any best practices you follow or technology you have in place, your data will always be exposed to some level of risk. However, if you adopt security best practices to secure your data, meet compliance requirements and get advice from a trusted security service provider when needed, you are already on the way to protect your brand, decrease your exposure to risk and improve your security posture.

[1] Computer Science and Telecommunications Board, National Research Council. "Computers at Risk: Safe Computing in the Information Age" (National Academy Press, 1991)

[2] Ponemon Institute (2016) "2016 Cost of Data Breach Study: Global Analysis"

[3] ibid.

[4] ibid.

[5] Reuters Investigates (2016) "Caribbean countries caught in crossfire of U.S. crackdown on illicit money flow." Available at: http://www.reuters.com/investigates/special-report/usa-banking-caribbean/ [Accessed: September 22, 2016]

[6] US Department of the Treasury (2016) "Resource Center – Foreign Account Tax Compliance Act (FATCA)". Available at: https://www.treasury.gov/resource-center/tax-policy/treaties/Pages/FATCA.aspx [Accessed: September 18, 2016]

[7] St. Lucia Times (2016) The CAB Encourages Caribbean Governments to Comply with FATCA". Available at: http://stluciatimes.com/2016/09/02/cab-encourages-caribbean-governments-comply-fatca [Accessed: September 18, 2016]

We are Massy Technologies InfoCom.

Your first choice partner, enriching the lives and experiences of all stakeholders through the delivery of Innovative Information and Communications Solutions.

Providing ICT Solutions, Support and Services in:

IT SOLUTION SALES

- ORACLE Enterprise Solutions
- Financial Services Solutions
- Servers and Storage Solutions
- Enterprise Content Management Solutions
- Industry-specific Solutions

BUSINESS COMMUNICATIONS

- SurePay Electronic Payment System
- LAN Infrastructure and Network Security
- Wireless Broadband (WAN) and Corporate ISP
- Voice and Data Networks
- PBX/IP Telephony
- Two-way Radio

BUSINESS PRODUCTS

- Desktops, Notebooks and Peripherals
- Office/Classroom Virtualisation Solutions
- Multi-functional Devices
- Managed Print Services
- Security Equipment

TECHNICAL SUPPORT SERVICES

- Pre and Post-implementation Support
- Testing and User Training
- Upgrades and Enhancements
- Ongoing System Monitoring and Preventative Support

PROJECT SERVICES

- Inventory Management
- Information Management
- Project Coordination and Administration
- ICT Strategy Consulting
- Business Transformation Management
- Risk Management and Business Continuity Planning

Partnered with:

Microsoft IBM IBM maximo TOPdesk INTERNET SECURITY SYSTEMS XCELLENET OPENTEXT SHARP ORACLE hp motorola EMC² AVAYA cisco NCR SAIC FILENET

MASSY TECHNOLOGIES
InfoCom

E: marketing.infocom@massytechnologies.com
W: www.massytechnologies.com/infocom