2ND NATIONAL CONFERENCE ON

CYBER SECURITY & DATA PROTECTION

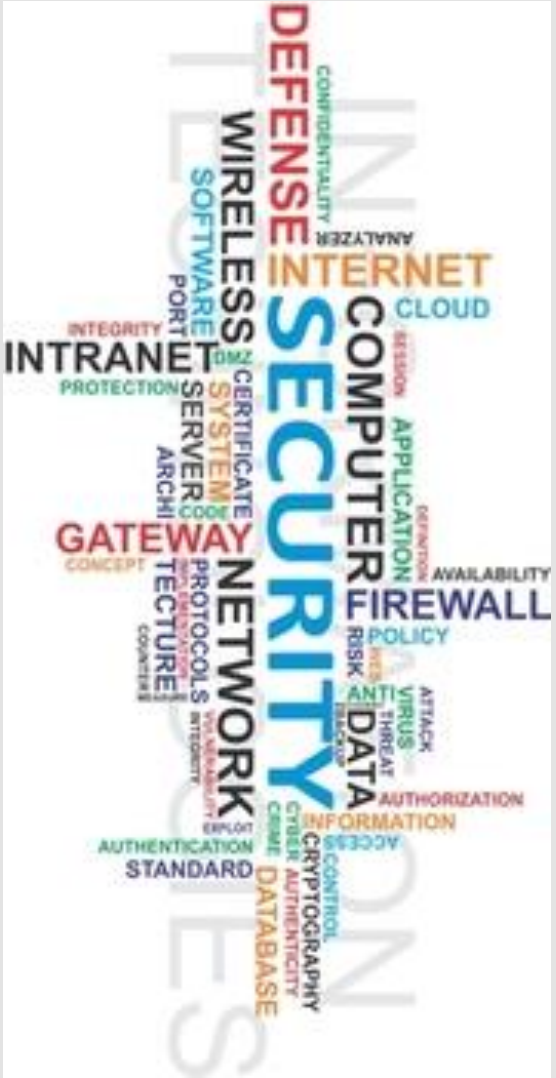
NATIONAL COMMERCIAL BANK JAMAICA LIMITED

Under Cyber-Attack!!!

MANAGING THREATS TO YOUR BUSINESS:

PUBLIC & PRIVATE SECTOR ORGANIZATIONS

PRESENTER: CECIL WILLIAMS



NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Agenda

- Threat Landscape
- Advanced Persistent Threats
- Breaches
- Current Attack Vectors
- Lessons
- Governance - Preventive measures
- SMEs and Awareness

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Threat Landscape

Which entities do cybercriminals target ?

- Governments
- Public Entities
- NGOs
- Private Organizations
- SMEs
- Individuals

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Threat Landscape

Who are the cybercriminals?

- Governments ?
- Private Organizations ?
- Individuals ?

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Threat Landscape

What do cybercriminals target / Why cybercrime?

- Classified government information
- Trade Secrets
- Financial and demographic data (Black Market sales)
- Personal data (User credentials /files/documents/pictures)
- Challenge/satisfaction of breaching highly secure systems

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

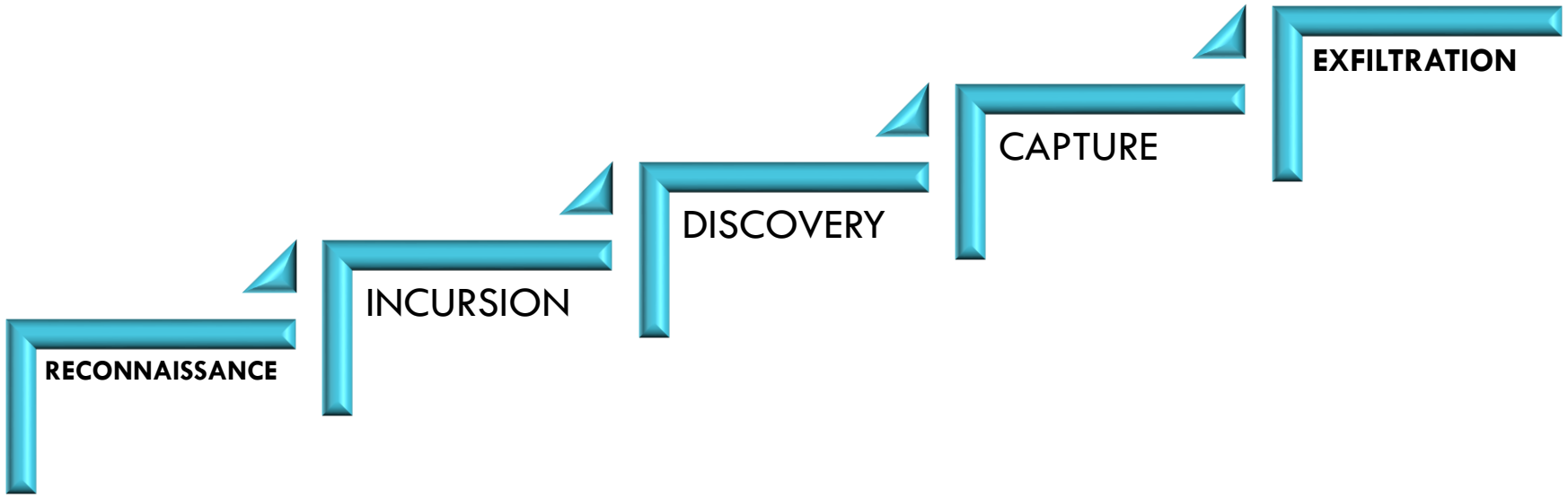
Threat Landscape:

Advanced Persistent Threat

(APT)

An advanced persistent threat (APT) uses multiple phases to break into a network, avoid detection, and harvest valuable information over the long term.

- Symantec



NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Threat Landscape:

Advanced Persistent Threat

(APT)

There are only a few groups globally that have the capability, skills, funding and infrastructure to launch an APT. Mainly nations are doing it.

Countries could include:

- **China**
- **Russia**
- **USA**

Little is known about other G20 Nations

The APT Toolkit

An attacker has a substantial arsenal of tools at the ready in order to launch and maintain their attack.

- Fortinet

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Breaches

TARGET

Data stolen

Credit and debit card numbers, expiration dates, the three-digit CVV security code, and even PIN data for 40 million account holders

Names, mailing addresses, phone numbers and emails of 70 million individuals

How the breach occurred

Login credentials stolen from a hired heating, ventilation and air conditioning company

Vulnerabilities:

Failure to properly segregate systems handling sensitive payment card data from the rest of its network (network segmentation).

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Breaches

JP MORGAN CHASE (July 2014)

Data stolen:

The accounts and contact information (names, addresses, phone numbers and emails) of 76 million households and 7 million small businesses

How the breach occurred

A list of open source applications and programs that run on JPMorgan's computers was obtained

Hackers breached the network via an employee's personal computer

The attack involved the use of malware

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Global Security Incident Trends

January – June 2014

Breaches

- Record-setting 1,331 reported data breaches exposing over 502 million records
- 39.6% of the breaches took place in the USA
- Individuals' user names, passwords and email addresses were exposed in more than 50% of reported incidents

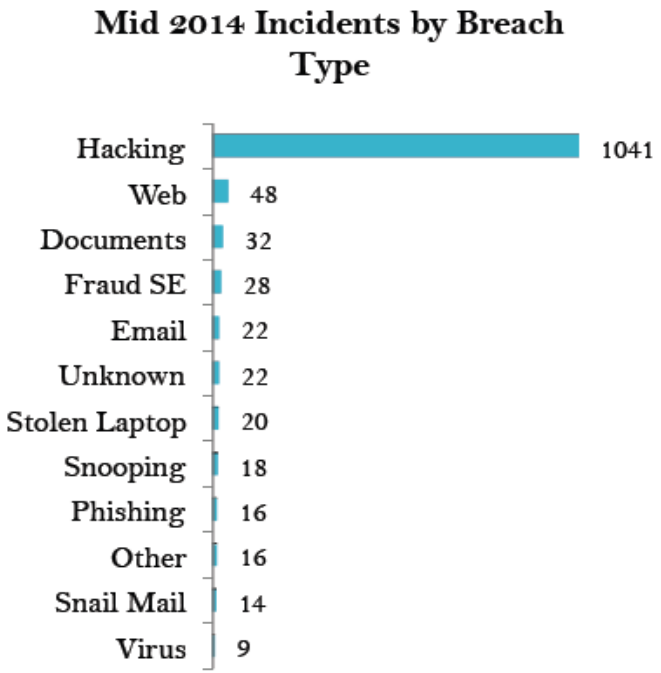
– Source: 2014 Mid-Year Data Breach QuickView Report, Datalossdb Open Security Foundation

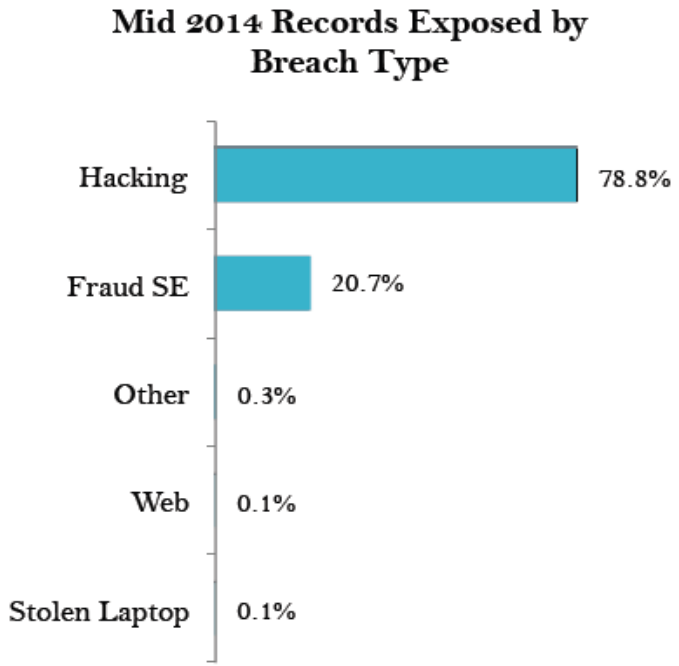
Global Security Incident Trends

January – June 2014

78% of all records compromised in the first half of 2014 were due to hacking.

Breaches





– *Source: 2014 Mid-Year Data Breach QuickView Report, Datalossdb Open Security Foundation*

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Breaches

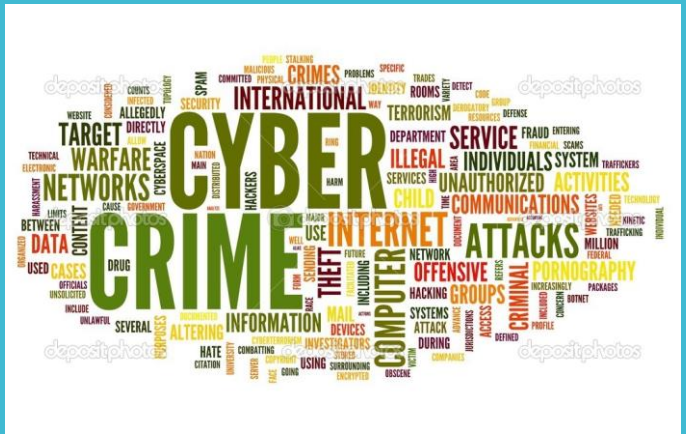
"If our largest and theoretically most capable organizations can't protect their systems, sooner or later all digital information is going to be untrustworthy. That means bank balances. It means deposits and withdrawals. It means the very system that keeps us safe and secure.

- Forbes.com

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Current Attack Vectors



Social Engineering

Using deception and manipulation to trick people into revealing their personal information. **Phishing** is a form of social engineering

Pharming

A form of online fraud very similar to phishing as pharmers rely upon the same bogus websites and theft of confidential information.

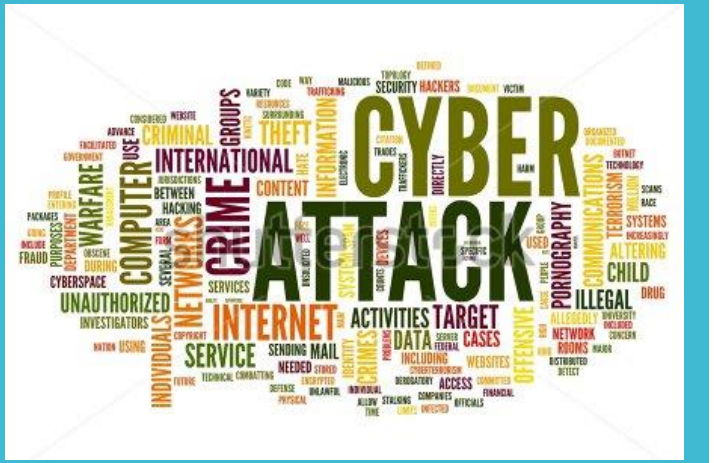
Keylogger, Form-Grabber Spyware

Attackers rely on data-capture malware, such as keyloggers, form-grabbers and other forms of spyware, to capture data directly from the user.

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Current Attack Vectors



SQL Injection

The SANS Institute has identified SQL injection errors as one of the most common errors in software.

Cross-Site Scripting (XSS) attacks

A type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites.

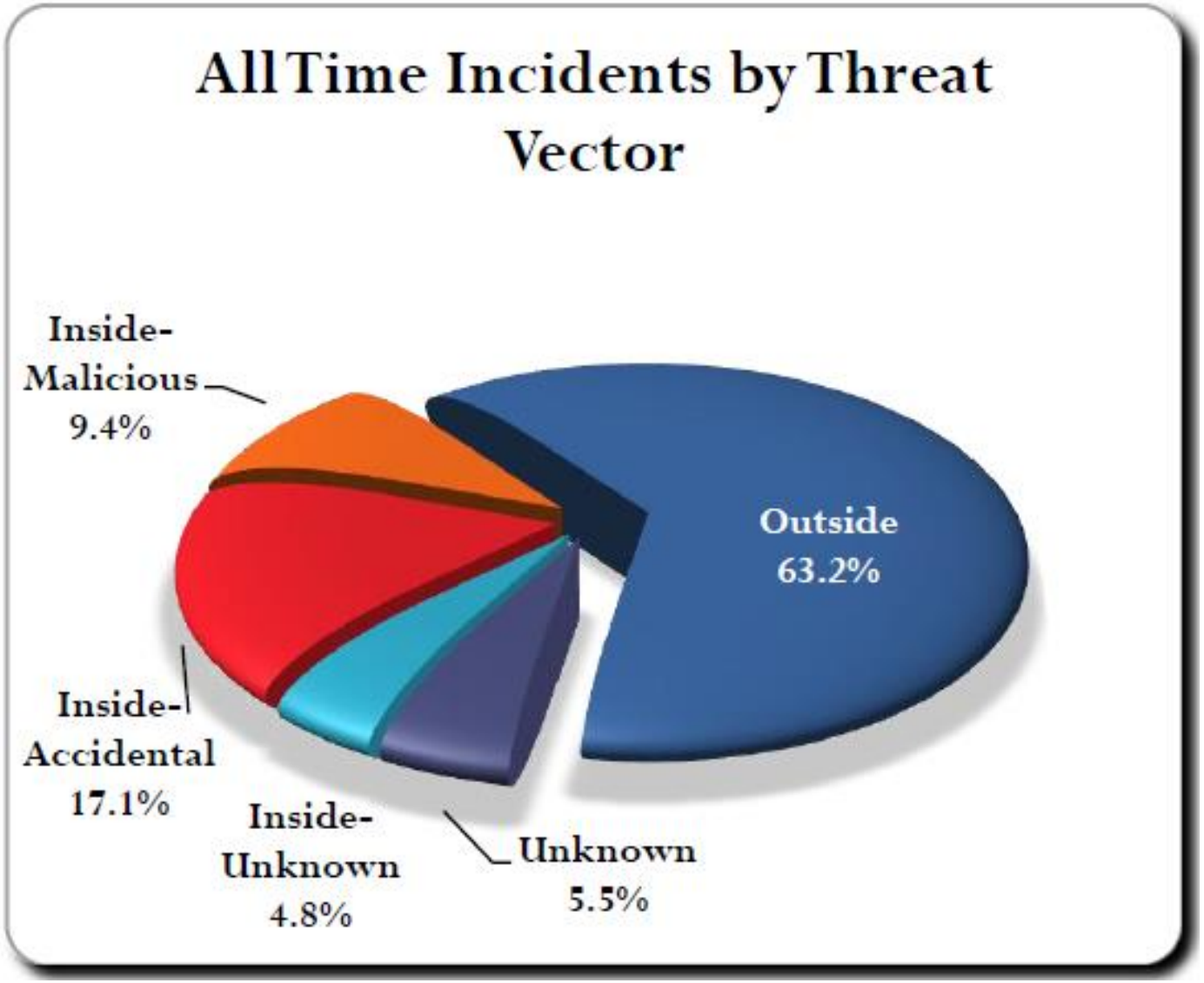
Man-in-the-middle attack

A form of active eavesdropping in which the attacker makes independent connections with the victims.

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Current Attack Vectors

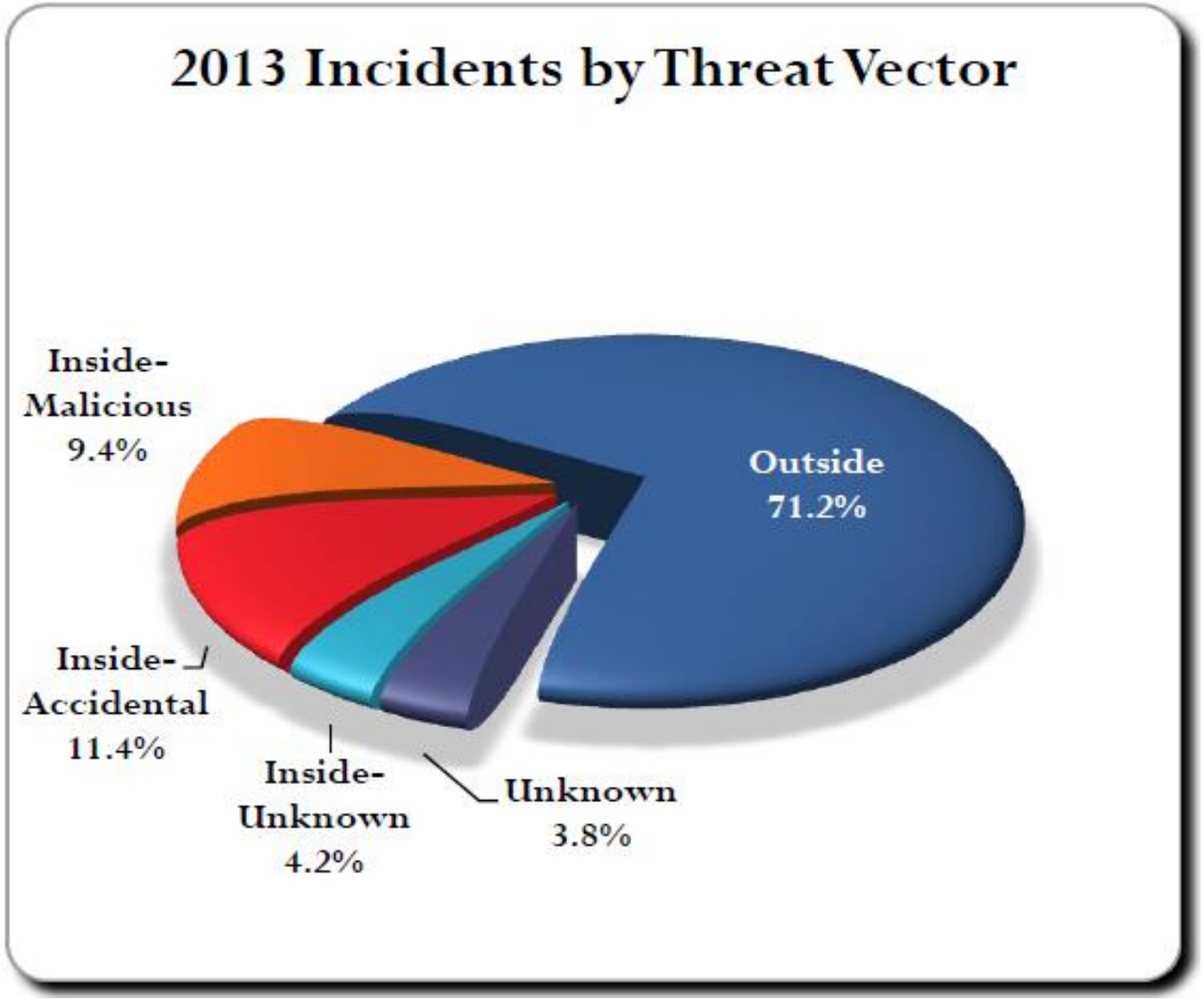


– Source: 2014 Mid-Year Data Breach QuickView Report, Datalossdb Open Security Foundation

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Current Attack Vectors



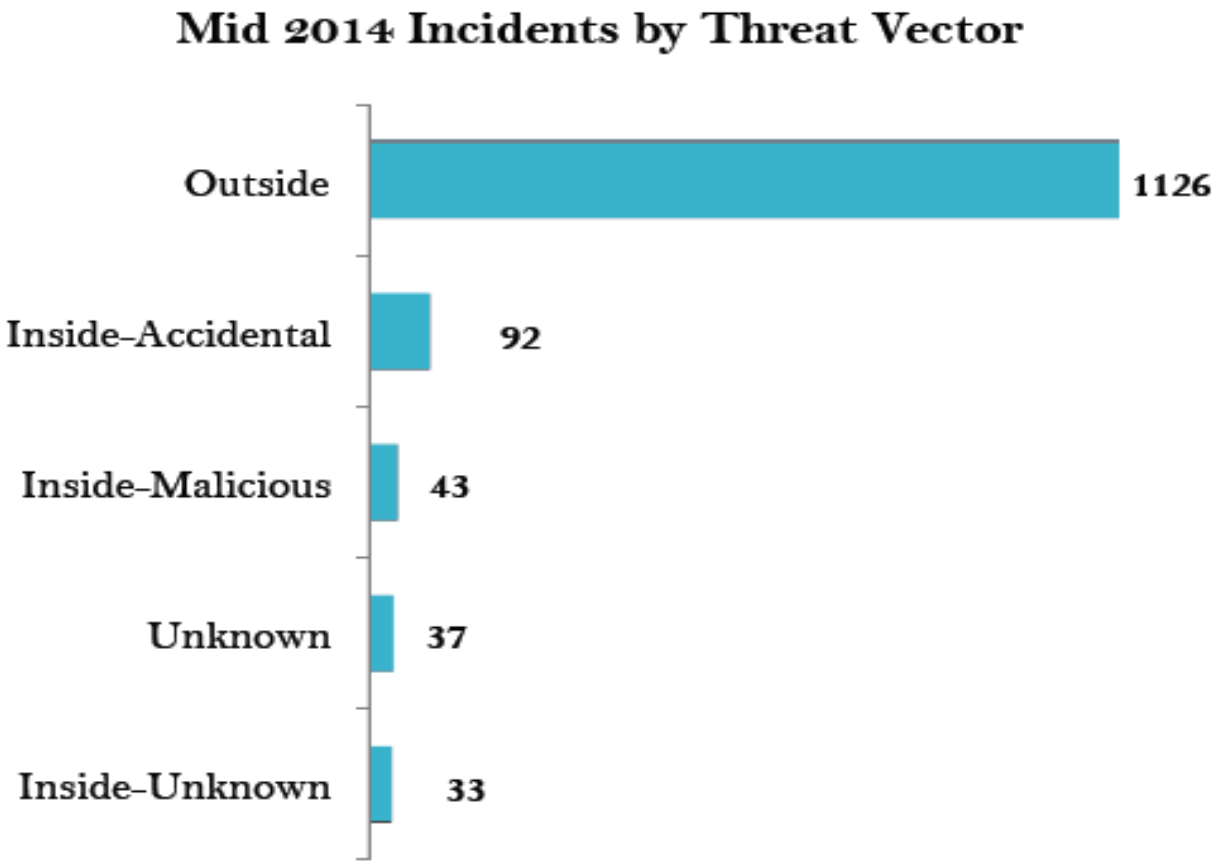
– Source: 2014 Mid-Year Data Breach QuickView Report, Datalossdb Open Security Foundation

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Current Attack Vectors

84.6% of incidents involved activity outside the organization



– *Source: 2014 Mid-Year Data Breach QuickView Report, Datalossdb Open Security Foundation*

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

Lessons

- Even with the best technologies ensure that the people and processes are also in place
- Pay attention to current attack techniques to address those specific threats as attackers are likely to use the same methods of attack again
- Sharing of attack intelligence is critical in combating cybercrime
- Pay attention to vulnerabilities that may be posed from open source applications and libraries.

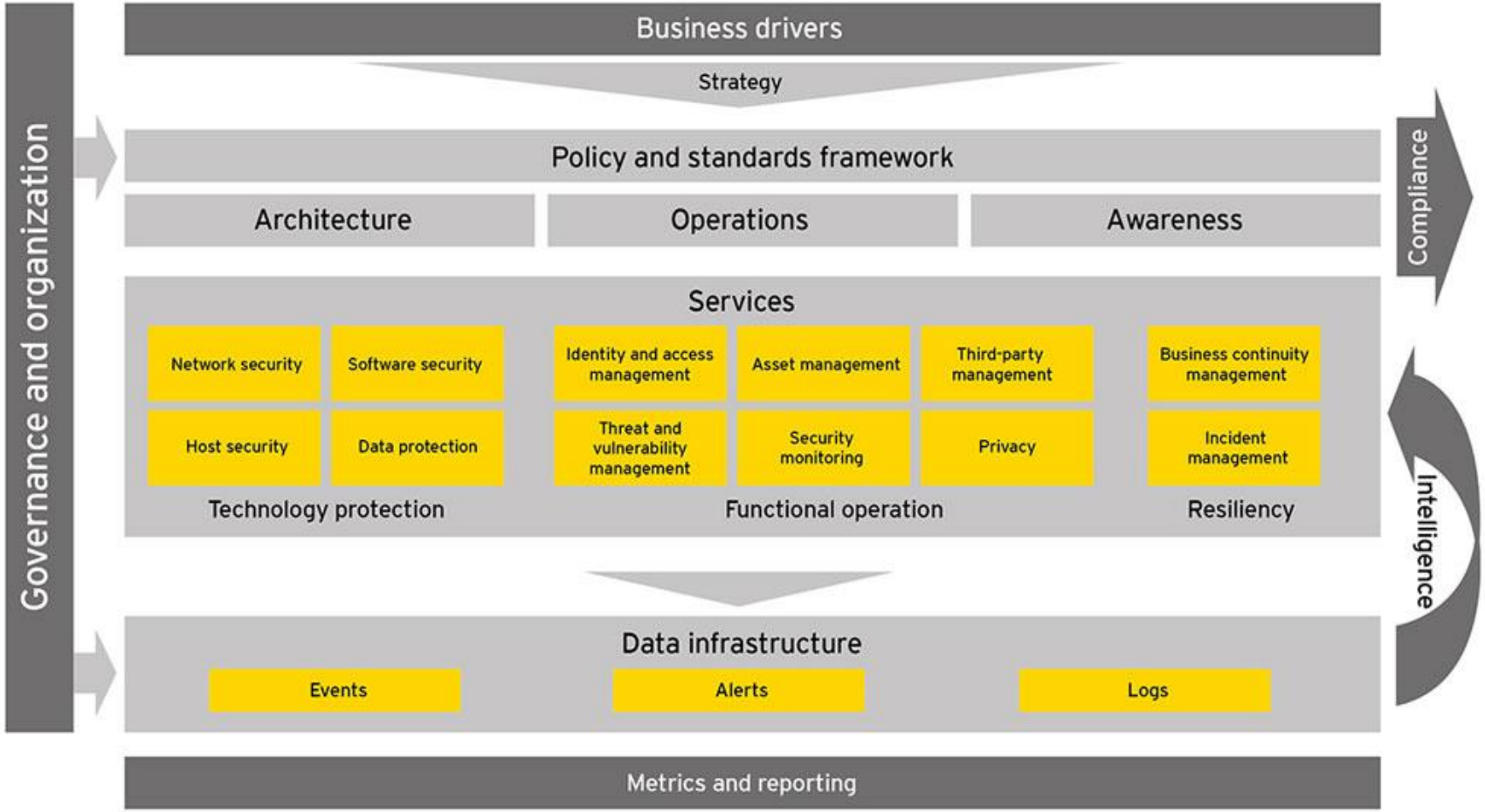
IT Governance

An organization must understand and be able to provide suitable responses to the following questions in order to have effective IT governance:

1. Does the organisation use an IT security framework?
2. How are employees made aware of their role related to cyber security?
3. How is IT security and IT governance managed within the organization?
4. What are the top 5 risks the organisation has related to cyber security?
5. Has the organization developed a robust response protocol?

The IT Governance framework must be underpinned by an effective Security Management framework which addresses Technology, Operations Procedure and Employee & Customer Awareness.

IT Governance



IT Governance:

Preventive Measures

As outlined in the framework special attention must be paid to the following areas to ensure the organization is proactively managing cybersecurity:

- End user awareness
- Customer Awareness
- Secure Coding Practices
- Patch & Vulnerabilities Management practices
- Segregation of Sensitive systems
- Greater security due diligence/auditing of third party suppliers/service provider
- Timely security incident monitoring & response procedures
- Using technologies i.e. Network Access Control to enforce organizations security policies
- Using technologies that can detect anomalies i.e. file integrity monitoring & heuristic anti-virus technology
- Ensure security code reviews are completed for all open source applications and libraries
- Complete thorough research for any technology products being acquired –particularly start-up companies, review reasonably priced cloud services.

SMEs and awareness

Cybercrime prevention can be straight-forward - when armed with a little technical advice and common sense, many attacks can be avoided.

In general, online criminals are trying to make their money as quickly and easily as possible and may target small and medium sized businesses. The more difficult you make their job, the more likely they are to leave you alone.

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

MONA ICT POLICY CENTRE UWI

SMEs and awareness

The tips below provide basic information on how you SMEs can protect themselves:

- Keep your computer current with the latest patches and updates (browser, software).
- Do not use free Wi-Fi and hotspots for business purposes.
- Make sure your computer is configured securely.
- Choose strong passwords and keep them safe.
- Protect your computer with security software. e.g. antivirus
- Protect your personal information.
- Review bank and credit card statements regularly.
- Use separate devices for business and entertainment

NATIONAL COMMERCIAL BANK JAMAICA LIMITED

QUESTIONS

MONA ICT POLICY CENTRE UWI