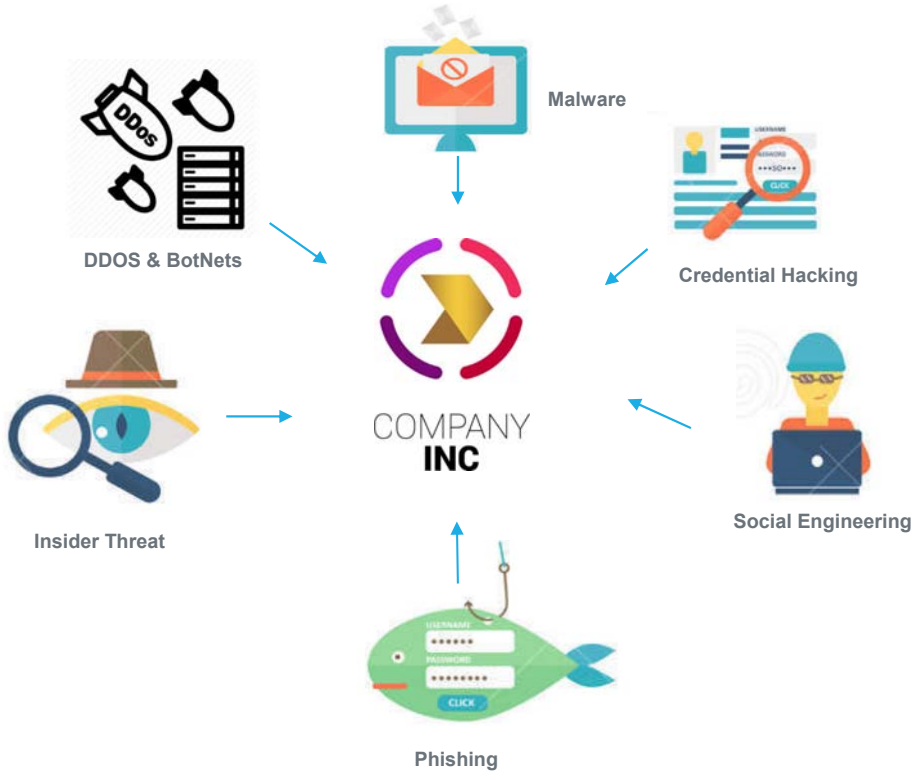
Key Strategies in Reacting to Cyber Incidents

Deyves Fonseca
Sr. Manager, Technology Risk & Governance
TD Bank

FEBRUARY 1, 2019




WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.
Dilbert.com DilbertCartoonist@gmail.com
WAIT FOR IT
Enter your bank account number.
SCAM.
5-19-14 ©2014 Scott Adams, Inc. /Dist. by Universal Uclick
THERE IT IS
Enter your bank account number.
OKEY-DOKEY.

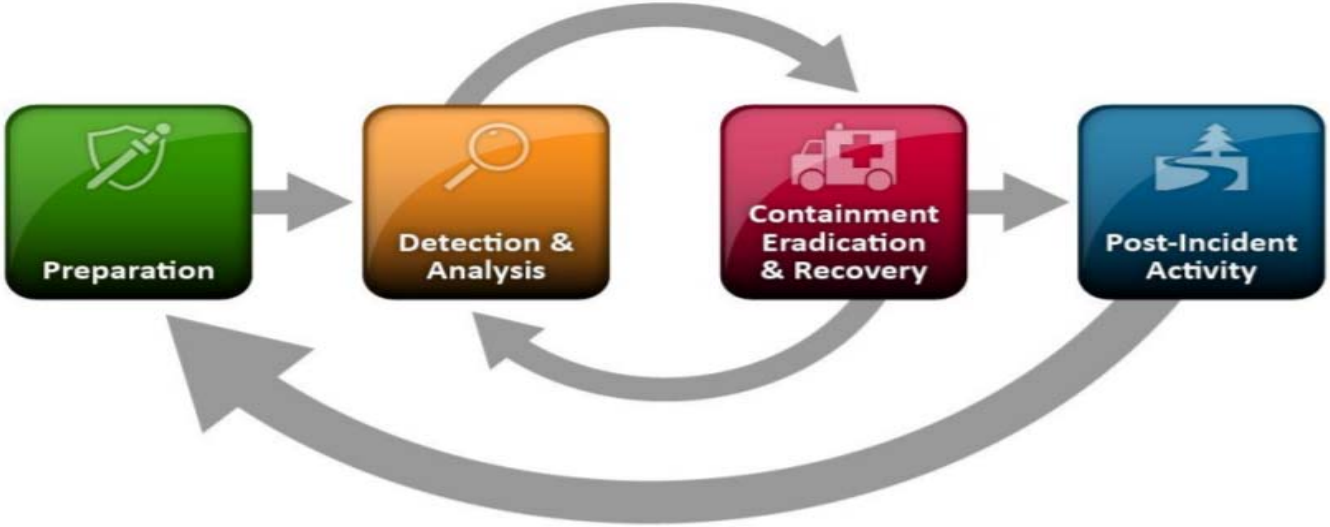
INTRODUCTION

- **Cyber Incident Response** is a key component of an effective cyber security program.
- Cybersecurity-related attacks have become more numerous and disruptive over time. New types of security-related incidents emerge frequently. **According to Positive Technologies, an Enterprise Security Solutions firm, there was a 47% increase in cyber attacks by Q2 2018 compared to 2017**.
- Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented**. In fact, a 24%* increase of unique cyber incidents was observed in Q3 2018 compared to 2017.**
- An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.
- This presentation will discuss a common framework used to handle cybersecurity incidents across the Industry, highlight some best practices and discuss some interesting Industry trends.

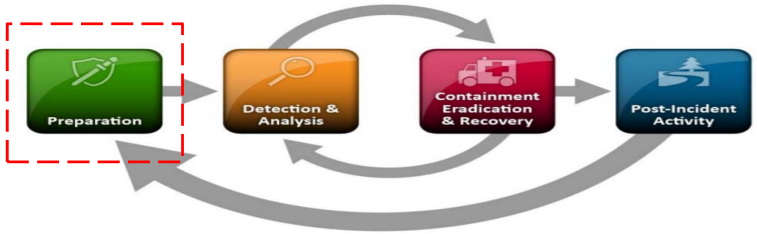
Business Strategy Alignment

Cyber Policy, Plan & Procedure Creation

Incident Response Life Cycle*



* Based on NIST SP-800-61 R2



Preparation

Primary Objectives of Cyber Incident Response

- ❑ Limit the Scope of the Attack (containment)
- ❑ Bring Business operations back to acceptable/regular services

What is a Incident ?

- ❖ Any event that has a negative effect on the Confidentiality, Integrity and Availability of an Organization's assets.

What is a Cyber Incident ?

- ❖ An incident that is result of an attack, or the result of malicious or intentional actions on the part of users.

Preparation

Communication

Prioritization & Severity of Incidents*

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

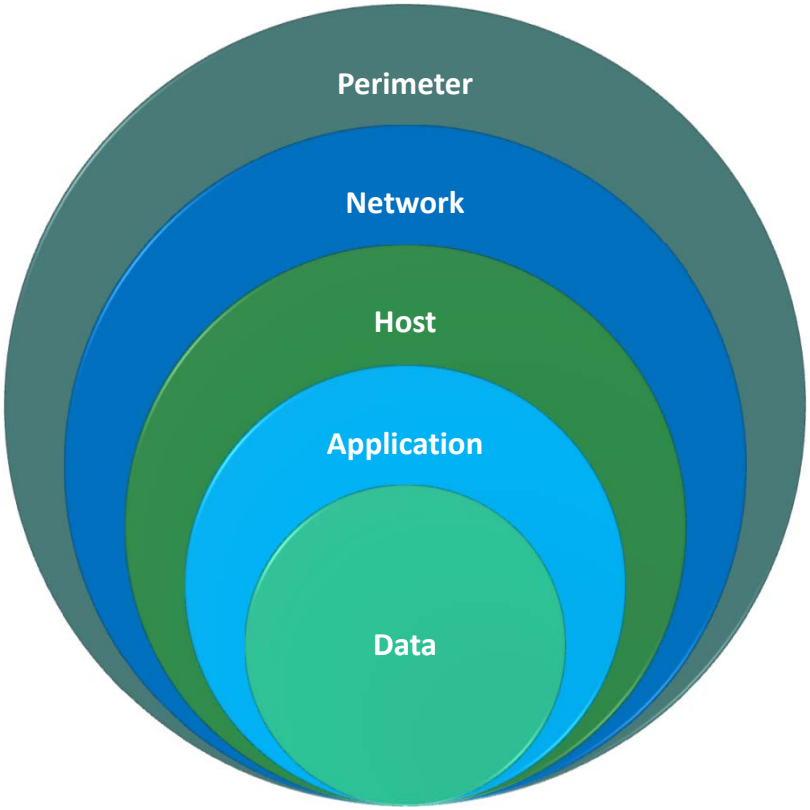
	Observed Actions	Intended Consequence[1]
Effect		Cause physical consequence
		Damage computer and networking hardware
Presence		Corrupt or destroy data
		Deny availability to a key system or service
Engagement		Steal sensitive information
		Commit a financial crime
Preparation		Nuisance DoS or defacement

* H-ISAC (US - Health Information Sharing Analytics Center)

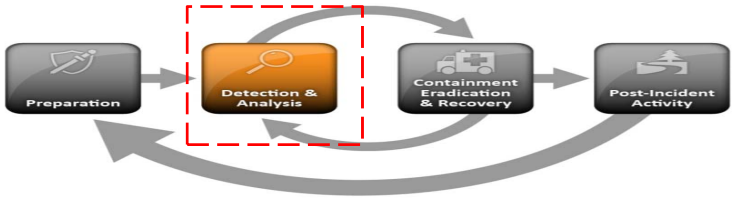
Preparation

Prevention is Key !

- Risk Assessment
- User Awareness & Training
- Host Security
- Network Security
- Malware Prevention
- Data Leak Protection
- Perimeter Security
- Scenario Analysis

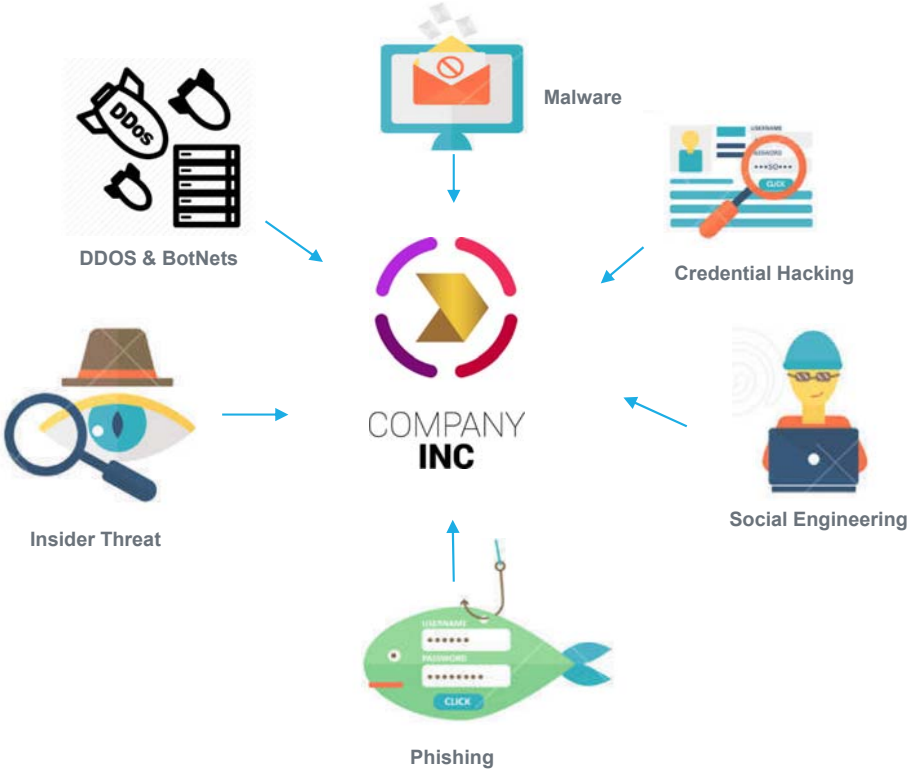


* InfoSec Institute – Defense In Depth

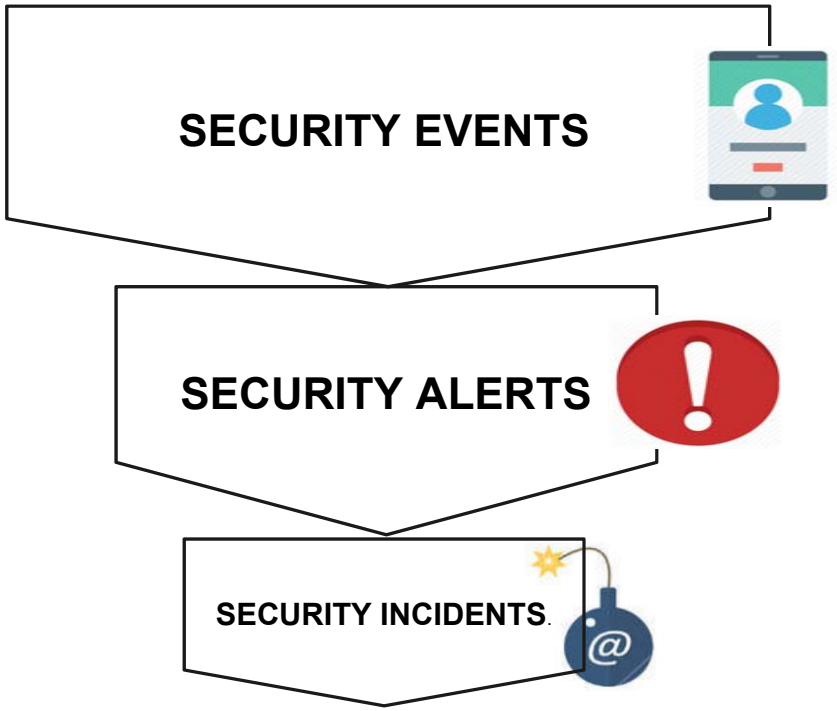


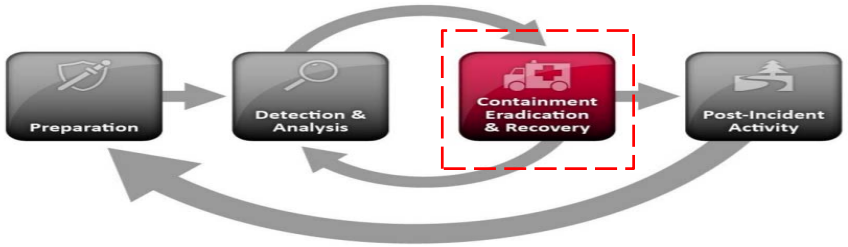
Detection & Analysis

Cyber Threats/Vectors Examples



Security Activity





Containment, Eradication & Recovery

Incident Prioritization & Notification

- ✓ What is the impact ?
- ✓ Was data breached ?
- ✓ What kind of data ?
- ✓ How difficult is recovery ?
- ✓ Who do I need to engage ?

Choose Containment Strategy

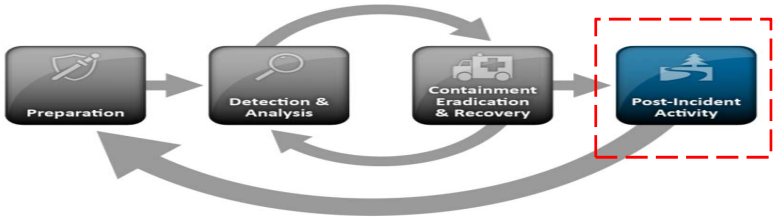
- ✓ What is the severity ?
- ✓ Do I need to invoke BCP (Business Continuity Plan)?
- ✓ Do I need to invoke DRP (Disaster Recovery Planning) capabilities ?

Evidence Gathering & Investigation

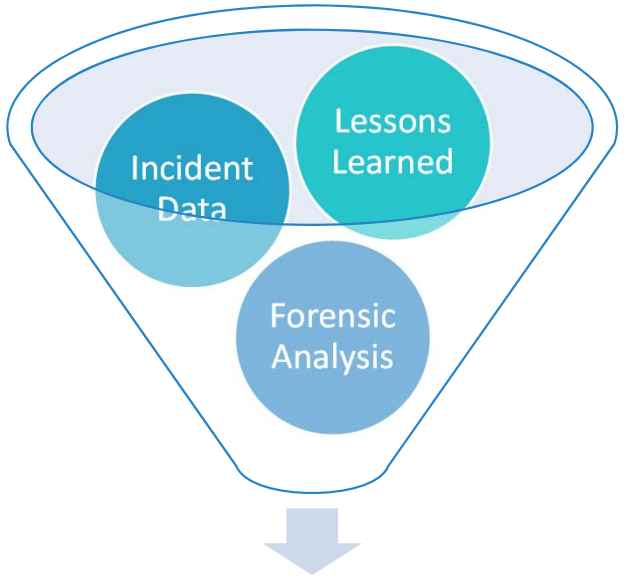
- ✓ What was the source of the attack ?
- ✓ Where did it come from, when ?
- ✓ Who was involved ?
- ✓ Is it happening elsewhere ?

Eradication & Recovery

- ✓ Is the incident contained ?
- ✓ Is the business operating normally ?
- ✓ Have we eradicated the root cause of the problem?
- ✓ Who was involved ?
- ✓ Is it happening elsewhere ?



Post-Incident Activity



Adjusted Systems & Processes

- ✓ How can we improve our handling process ?
- ✓ Do we need to adjust our security policies ?
- ✓ How much did the incident cost ?
- ✓ Would investment in new security products outweigh costs ?

Cyber Statistics & Trends*

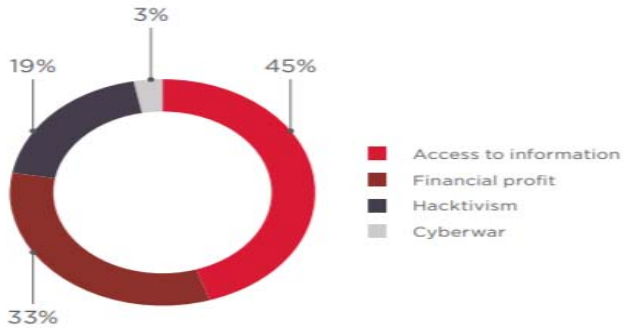


Figure 1. Attackers' motives

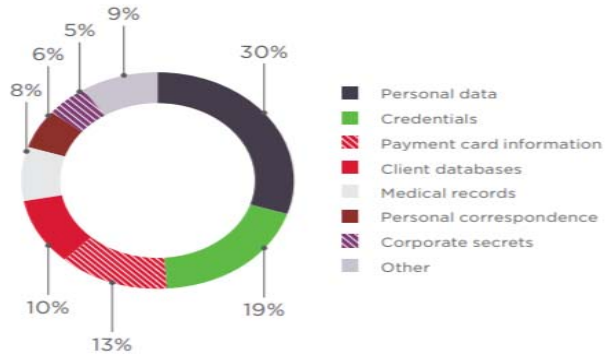


Figure 2. Types of stolen data

Attacker Motives (Fig. 1)

- Data Theft is on the rise
- It is easier for adversaries to steal private data, commercial secrets than steal money in cyber space.

Types of Data Stolen (Fig. 2)

- Private Data
- Credentials
- Payment Card Information

* Positive Technologies Cybersecurity Threatscape Q3 2018

Cyber Statistics & Trends*

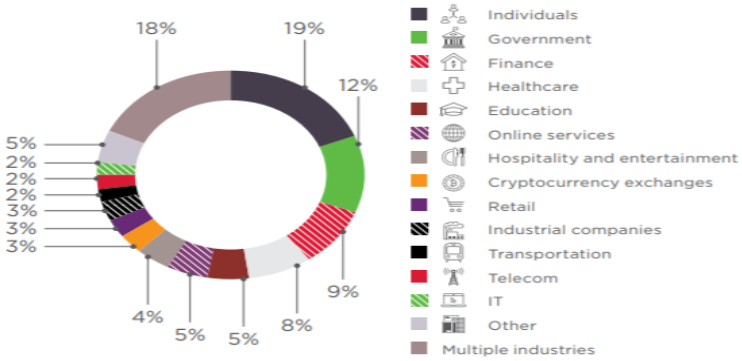


Figure 3. Victim categories

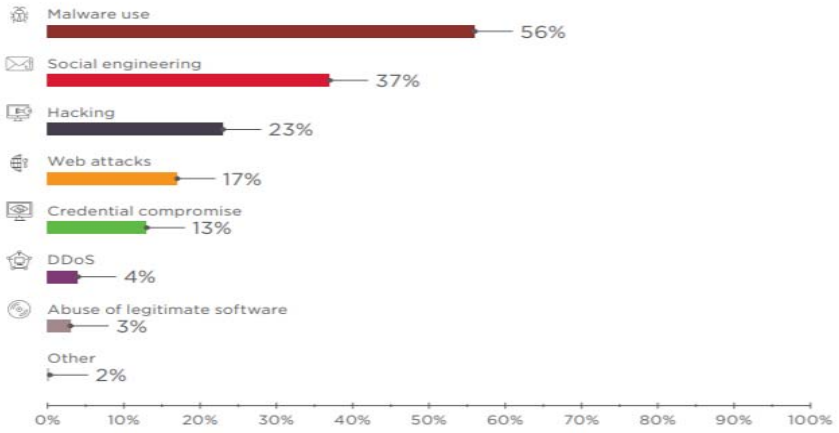


Figure 4. Attack Methods

Victim Categories (Fig. 3)

- Individuals
- Government
- Finance

Attack Methods (Fig. 4)

- Malware
- Social Engineering
- Hacking

* Positive Technologies Cybersecurity Threatscape Q3 2018

Cyber Statistics & Trends*

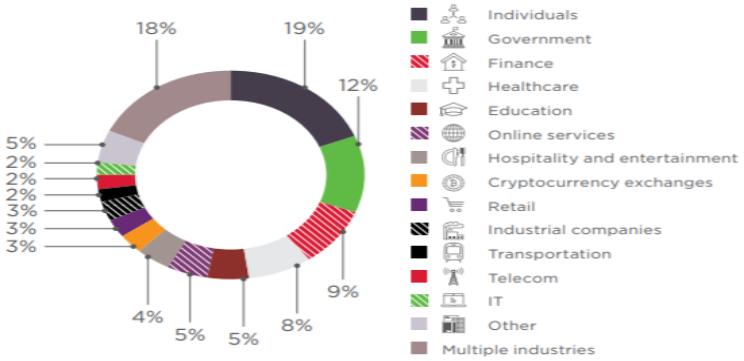


Figure 3. Victim categories

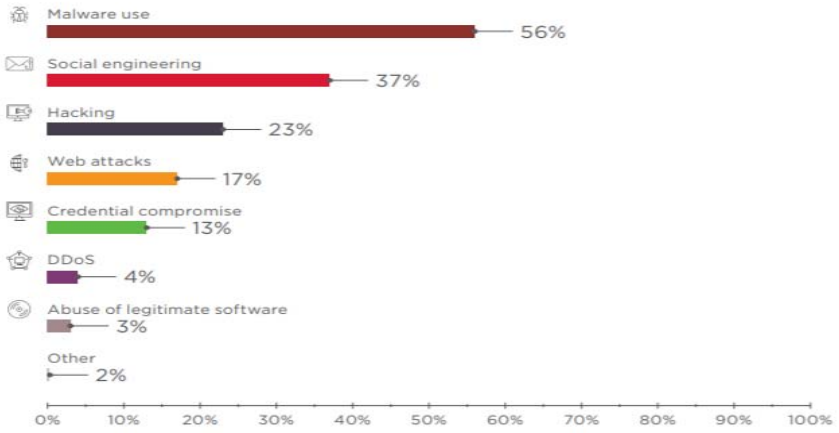


Figure 4. Attack Methods

Victim Categories (Fig. 3)

- Individuals
- Government
- Finance

Attack Methods (Fig. 4)

- Malware
- Social Engineering
- Hacking

* Positive Technologies Cybersecurity Threatscape Q3 2018

IN CONCLUSION…….

- **Cyber Risk is a business problem. Everybody has a role to play !**
- Start with the basics: Focus on *Inventory of Assets, Continuous Vulnerability Management, Secure Configuration, Access Management (Least Privileged), Maintenance, Monitoring & Analysis of Audit Logs and of course User Awareness and training*…. It would protect organizations from the most basic vulnerabilities and threats.
- Perform periodic risk assessments in your environment: Prevention is far less costly than remediation.
- Ensure your organization has the necessary tools and process in place to detect, analyze, respond and recover from cyber incidents.
- Cyber Incident Management needs to evolve continuously in order to better prepare to the ever changing cyber landscape.