Importance of Cyber Security Control Automation

Introduction:

Hackers, Attackers, Viruses, key loggers and Malicious programs can access the company system in different ways due to multiple system weakness.

Attackers, who could be located anywhere in the world, are continuously scanning the company details address space of target organizations, once they gain access to computer, they can cause serious data breach.

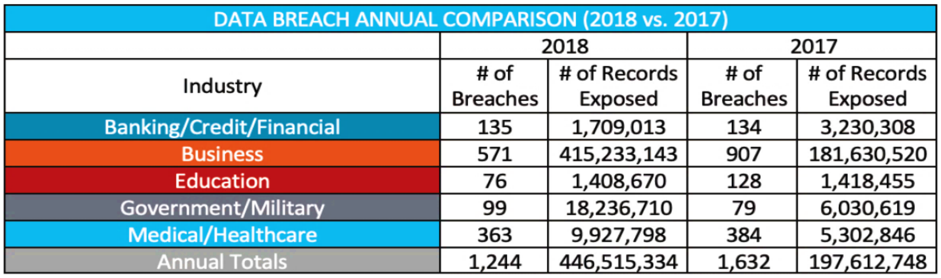
Damage from a malware intrusion can take many forms, from the loss of important data to serious financial consequences.

The global cost of cybercrime has now reached as much as $600 billion — about 0.8 percent of global GDP.

As per data breach report, the number of consumer records containing sensitive personally identifiable information (PII) jumped **126 percent** from 2017 to 2018.

2017 – 196,612748 records are breached

2018 – 446,515334 records are breached



DATA BREACH ANNUAL COMPARISON (2018 vs. 2017)				
	2018		2017	
Industry	# of Breaches	# of Records Exposed	# of Breaches	# of Records Exposed
Banking/Credit/Financial	135	1,709,013	134	3,230,308
Business	571	415,233,143	907	181,630,520
Education	76	1,408,670	128	1,418,455
Government/Military	99	18,236,710	79	6,030,619
Medical/Healthcare	363	9,927,798	384	5,302,846
Annual Totals	1,244	446,515,334	1,632	197,612,748

Source : https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf

Data Breach Impacts:

Examples:

$5 Billion Fine
Facebook

1. US Federal regulators have fined Facebook US$5 billion for data breach & privacy violations.

2 UK's ICO (Information Commissioner's Office) have fined British Airways £183.39 Million under the General Data Protection Regulation (GDPR) breach.

$57 Million Fine
Google

3.ICO have fined of £99,200,396 ($123 Million) on international hotel chain Marriott for November of 2018 data breach under the General Data Protection Regulation (GDPR) act.

Professional Risk:

CISO's (chief information security officer) are accountable for **data security** and must provide confidence to investors, executives, external auditors, and regulators that personal information is secure.

His responsibility to ensure that the information security controls set in place are operational as per defined process.

The study involved 612 CISOs, CIOs, and other information security professionals. Surprisingly 45% stated that they worry about losing their jobs in the aftermath of a major cyber-attack.

A survey conducted at "Infosecurity" Europe. In this study, security professionals were asked which company position was most responsible in the event of a company data breach.

Of the respondents,

40% believed that the CEO would be first on the firing line

- followed by the CISO (21%)
- “Other” (15%)
- CIO (14%)

Framework for Preventing Cyber Attacks

Cyber security is a sub-section of Information Security. Three pillars (**People, Processes and Technology)** are important to build Effective Information Security Management System (ISMS)

People
Process
Technology

People There are two key element need to be consider.
1. An effective security awareness programs can help reduce the risk of cyber threats targeted at exploiting people.
2. Updated skills and qualifications are required for security staff to ensure that appropriate controls, technologies and practices are implemented to succeed the latest cyber threats.

Process
It is the key to the implementation of an effective cyber security strategy. Processes are crucial in defining how the organisation’s activities, roles and documentation are used to mitigate the risks to the organisation’s information.

Technology

It is important & critical to cyber security. Its involves putting the right systems in place to processes and make them effective.

Risk Management:

Risk Management is the process to identify, assess and manage the threats to an organization's data, systems, networks, and infrastructures.

It involves identifying management risks and vulnerabilities and applying appropriate actions and solutions to make organization is adequately protected.

There are multiple cyber security frameworks and standards like NIST, ISO/IEC 27001, COBIT etc., which provides a common language to understand, manage the risk.

The frameworks and standards can be used to help identify and prioritize actions for reducing cybersecurity risks and regulators compliance requirements like SoX, PCI, HIPAA, FFIEC, FISMA, NERC-CIP, SWIFT, GDPR, CDM, CJIS etc.,

IDENTIFY RISK
ASSESS RISK
MANAGE RISK

For Example, the NIST framework explains the way to Identify, Protect, Detect, Respond, to the cyber risks.

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Risk identification is the initial step in the cyber security risk management that involves identifying specific elements of the three components of risk: **Assets, Vulnerabilities and Threats.**

Identification of Assets:

Hardware asset inventory is the **fundamental requirement** for managing cyber-risk. In general, the majority of organisations are not managing their IT hardware asset inventory.

The key requirement across any organisation is to manage the asset inventory.

you can't manage what you can't see. Similarly: if you can't see it, you can't secure or manage your cyber-risk.

There are multiple tools that can be used to build a primary asset inventory of systems connected to an organization's network.

Identification of Vulnerabilities:

The purpose of vulnerability analysis is to find out current exposure, whether existing safe guards are sufficient to manage in terms of **confidentiality, integrity or availability.** There are various tools (ex: Nessus, Sara) can be used to identify specific vulnerabilities in systems.

As per National Vulnerability Database, the vulnerability per year is

- Over 70 million hits per year
- 29,000 vulnerabilities
- About 20 new vulnerabilities per day

Identification of Threats:

Threats can be defined as anything that would contribute to tampering, destruction or interruption of any service.

The threat analysis takes care of each element of risk that could possibly happen. These threats can be split into Human and Nonhuman elements.

Human: Hackers, Theft (electronically and physically), Non-technical staff, financial/accounting), Accidental, Inadequately trained IT staff, Backup operators, Technicians etc.,

Nonhuman: Viruses, Floods, Fire, Electrical, Air (dust), Heat control.

Goals of Risk Analysis:

The aim of conducting a risk analysis is to identify an **acceptable risk level**.
A risk analysis has four main goals:

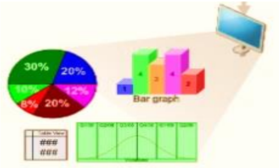
- to identify assets and their values.
- to identify vulnerabilities and threats.
- to analyse the probability and business impacts of threats.

to provide commercial balance between the impact of the threat and the cost of the countermeasure.

Cyber Security Control Automation:

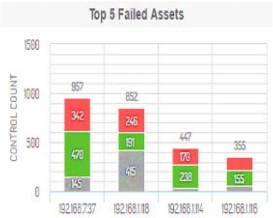
Cyber Security Controls have become an outline to help Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) to deploy the most effective processes and tools to secure computer systems according to risk.

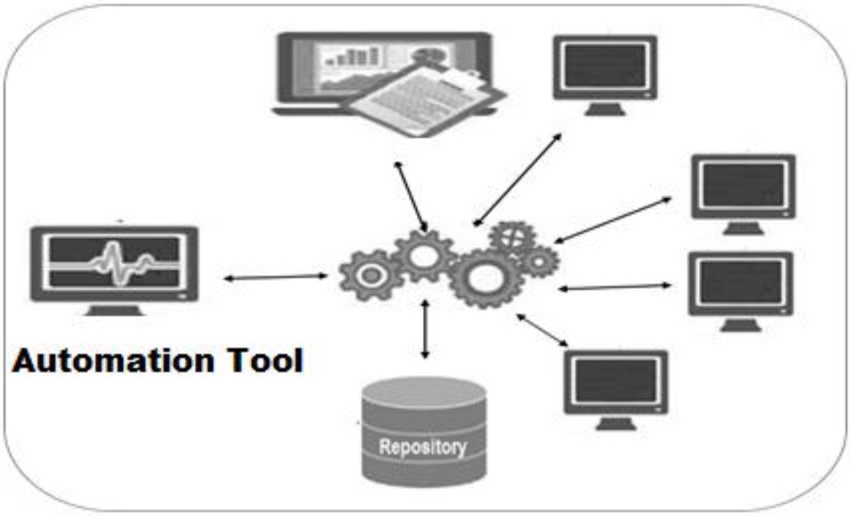
By following any of the Framework / Guideline (NIST /COBIT / ISO), organization can reduce or protect the cyber risks.



Organizations can use automation tool to control testing approaches where a tool is run on the systems (desktops/laptops/servers etc.,) to download control data from tables and structures and algorithms are stored in the repository to read controls to start the automation process.

Asset Data Collections





The following example will show how automation tool can be used to automate controls:

<u>Security Control:</u>
<u>EX: ISO 27001 A. 8.1.1 and PCI 2.4</u>

Inventory of Assets Control:

-All assets should be clearly identified and an inventory of all important assets drawn up and maintained. (ISO 27001)

-Maintain an inventory of system components that are in scope for PCI DSS

Implementation Guidance:

An organization should be able to identify all critical assets and document the importance of these assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets should be identified.

Automation tools can be used to produce an automated, complete inventory of systems on the network. This tool scans any IP enabled device, including servers, desktops, laptops, routers, switches and firewalls.

Keeping track of IT assets and automatically identify whether unapproved or harmful software or hardware is installed.

Linking Configuration to Compliance and Cyber Security Control
<title>Asset Management </title>
<reference>ISO 27001: 8.1.1</reference>
<reference>PCI 2.4 </reference>

Automation tool makes it easier to see where potential risks may exist, so they can be prevented before major problems arise. such as illegal/unauthorized software, outdated software and unauthorized/malicious downloads.

Keeping systems and assets compliant will help to prevent / reduce cyber threat and support compliance requirements.

Authored by Monfort M,
TCS Cyber Security