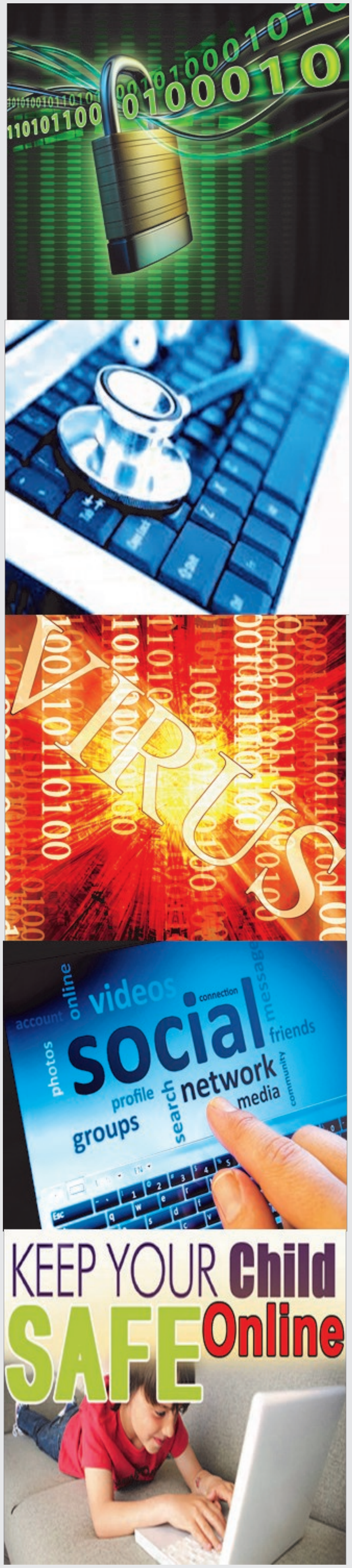
# CERT-MU E Security Newsletter

Volume 8 | Issue 1 | August 2018

## Inside this Issue:



CERT–MU

# Computer Emergency Response Team of Mauritius (CERT-MU)

## Your Partner in Cyber Security

## CERT-MU SERVICES

**Reactive Services:**

- ⇒ Incident Handling
- ⇒ Vulnerability Scanning and Penetration Testing

**Proactive Services:**

- ⇒ Dissemination of Information Security News, including virus alerts, advisories, vulnerability notes and warnings on latest cyber-attacks
- ⇒ Awareness campaigns on different Information Security themes for corporates, youngsters and the public in general
- ⇒ Organisation of international events such as Safer Internet Day and Computer Security Day
- ⇒ Organization of professional trainings on Information Security areas
- ⇒ Provision of educational materials through publications (includes guidelines, e-security newsletters, brochures, booklets, flyers) and a dedicated cyber security portal

**Security Quality Management Services:**

- ⇒ Assistance to organisations for the implementation of Information Security Management System (ISMS) based on ISO 27001.

## Cyber Security Portal

The Cyber Security Portal (http://cybersecurity.ncb.mu) is an initiative of CERT-MU to sensitise and raise awareness of the general public on technological and social issues facing Internet users .

The Portal consists of Internet best practices for:

- ⇒ Organisations
- ⇒ Parents
- ⇒ Kids
- ⇒ Home users

Dear Readers,

Greetings from CERT-MU and welcome to this eSecurity Newsletter.

We are pleased to inform you that CERT-MU has launched the Mauritian Cybercrime Online Reporting System (MAUCORS). The system is a national online system that allows the public to report cybercrimes occurring on social media securely. It also provides advice to help in recognising and avoid common types of cybercrime which takes place on social media websites. MAUCORS is operational since March 2018. This e-security newsletter introduces you to the system, its features and the benefits of reporting incidents on MAUCORS.

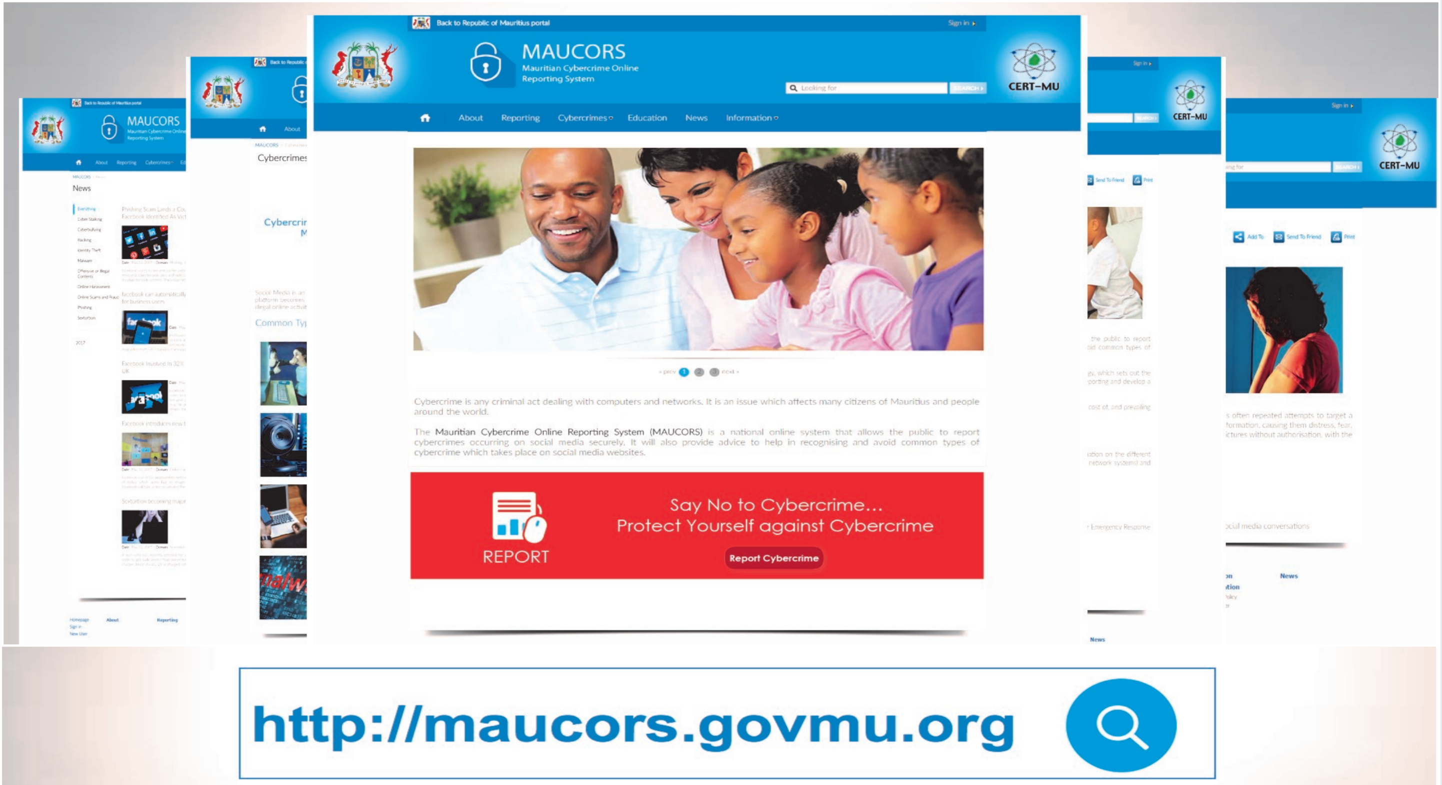
Our second article covers the General Data Protection Regulation (GDPR) from an IT Security Perspective. The GDPR is a regulation that requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The Data Protection Act 2017 of Mauritius has been aligned with the GDPR. This e-Security newsletter focuses on the GDPR from an IT Security Perspective. The emphasis is laid on the various aspects which link the GDPR with information security.

Other issues highlighted in this e-security newsletter include CERT-MU events, the latest information security news, best practices and tips.

We hope that you will find the articles interesting and enjoy reading!

**CERT-MU Team**

# Introducing: The Mauritian Cybercrime Online Reporting System (MAUCORS)



Back to Republic of Mauritius portal

Sign in

MAUCORS
Mauritian Cybercrime Online Reporting System

Looking for

SEARCH

CERT-MU

About · Reporting · Cybercrimes · Education · News · Information

« prev 1 2 3 next »

Cybercrime is any criminal act dealing with computers and networks. It is an issue which affects many citizens of Mauritius and people around the world.

The Mauritian Cybercrime Online Reporting System (MAUCORS) is a national online system that allows the public to report cybercrimes occurring on social media securely. It will also provide advice to help in recognising and avoid common types of cybercrime which takes place on social media websites.

REPORT

Say No to Cybercrime…
Protect Yourself against Cybercrime

Report Cybercrime

http://maucors.govmu.org

Cyberspace has grown exponentially around the world. Mauritius too has witnessed a significant rise in internet activities. Such phenomenal growth in access to information and connectivity has on one hand empowered individuals and organisation and on the other hand, posed new challenges to government and citizens. The risks of operating in the cyber world are reaching unprecedented levels as newer forms of threats and vulnerabilities continue to emerge. Such threats are becoming harder to predict as well as targeted in nature. With the ever-shrinking difference between the cyber and physical world  and the use of a large number of internet-connected devices, threat actors are seemingly well-positioned to cause disruption to a nation's government, businesses and citizens alike. As technology continues to offer numerous benefits to society, a number of divergent scenarios continue to stifle its widespread adoption and growth. Cybercrime has established itself as a fast growing area of crime. To prevent such misuse of information and communications technology (ICT) for criminal activities, a coordinated effort involving the government, businesses, citizens is required as well as the collaboration of international agencies.

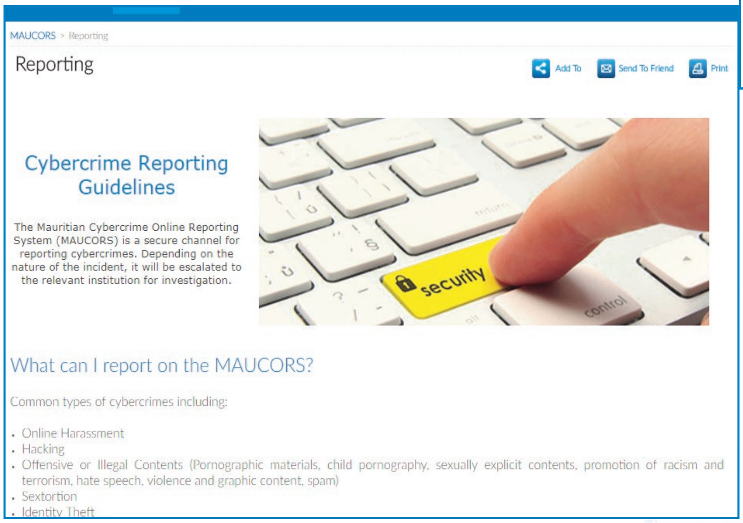
Making the cyber world safer is of primary interest to the government. Putting up deterrent measures against cybercrime is essential to the national cybersecurity as well as for protecting critical infrastructure of the nation. Enforcing data security measures and creating proactive security monitoring capability are vital for an organization to maintain a lead over emerging threats and protect their financial intellectual and customer-related information. A number of initiatives are being adopted and taken by the government to detect, prevent, investigate and prosecute cybercrimes. In line with this, the Mauritian Cybercrime Online Reporting System (MAUCORS) (http://www.maucors.govmu.org) has been established and is operational since March 2018.

**The Need for MAUCORS**

MAUCORS is one of the key initiative of the National Cybercrime Strategy that sets out the government's approach to combat cybercrime in Mauritius. MAUCORS is a centralised system that connects the Computer Emergency Response Team of Mauritius (CERT-MU), the Cybercrime Unit (Mauritius Police Force), the Data Protection Office and the Information Communication Technologies Authority (ICTA). The system allows citizens  to report social media incidents on one platform that can reach out the respective institutions.

In the light of the growth of the ICT sector in Mauritius, providing the right focus for creating a secure computing environment has become one of the compelling priorities for the country. Cyber space is vulnerable to a wide variety of threats which could hamper economic, public health, safety and national security activities. Reputation, trust and brand value can all be seriously affected by information loss and theft. However, with rapid identification, information exchange, investigation and coordinated response and re-mediation, the damaged caused by malicious activities can be mitigated.

It has been noted that often people do not know where to report an incident or which institution to seek assistance. In most cases, they go to the local police stations to make complaints. Citizens are then channeled to the institutions. Many instances of cybercrime also go unreported because victims either do not know where to report or do not think that it is worth reporting or even are reluctant to do so.



MAUCORS > Reporting

Reporting

Cybercrime Reporting Guidelines

The Mauritian Cybercrime Online Reporting System (MAUCORS) is a secure channel for reporting cybercrimes. Depending on the nature of the incident, it will be escalated to the relevant institution for investigation.

What can I report on the MAUCORS?

Common types of cybercrimes including:

- Online Harassment
- Hacking
- Offensive or Illegal Contents (Pornographic materials, child pornography, sexually explicit contents, promotion of racism and terrorism, hate speech, violence and graphic content, spam)
- Sextortion
- Identity Theft

MAUCORS was developed by CERT-MU to facilitate incident reporting. The system acts as an online one-stop shop for reporting incidents such as online harassment, identity theft, cyber bullying, sextortion, online scams, etc..

**MAUCORS Incident Reporting Process:**

The incident reporting process of MAUCORS is described below:

⇒ The victim log on http://maucors.govmu.org and report an incident

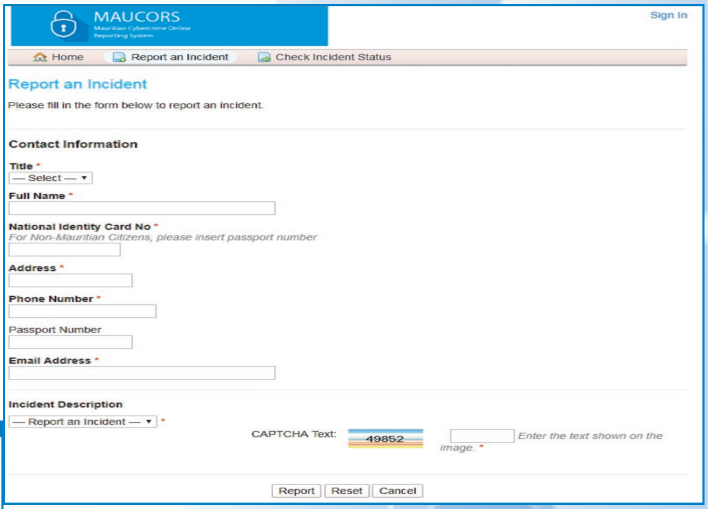
⇒ The victim receives an acknowledgement on screen and by email, along with a ticket number

⇒ CERT-MU receives the incident with all details

⇒ CERT-MU analyses the incident

⇒ Based on the nature of the incident, it is escalated to the respective agencies for further investigation and actions

⇒ The victim is notified about the incident escalation and which institution is handling the incident.



Report an Incident

Please fill in the form below to report an incident.

Contact Information

Title *
— Select — ▾

Full Name *

National Identity Card No *
*For Non-Mauritian Citizens, please insert passport number*

Address *

Phone Number *

Passport Number

Email Address *

Incident Description

— Report an Incident — ▾ *

CAPTCHA Text: 49852 *Enter the text shown on the image.* *

Report Reset Cancel

⇒ Incident is handled and resolved

⇒ The user is informed about the outcome of the incident

⇒ The incident is closed

**MAUCORS — Digitalisation**

MAUCORS is an example of digital and business transformation whereby different agencies are working together on one platform to meet citizens needs efficiently. The relevant institution has access to the system and works in an independent way of resolving the incident. The incident handling process and actions taken to resolve the incident are clearly defined and noted. MAUCORS also has lots of features that help the institutions to coordinate and resolve incidents effectively. For example, a dashboard which organises and presents the information in a way that is easy to read. Reports can also be extracted based on different parameters. This allows analyzing social media incident trends and patterns in the country as well as carry out risk profiling. The statistics gathered by MAUCORS allows authorities to have a national cybercrime picture of the Mauritian cyberspace.

## Common Types of Cybercrimes on Social Media

Online Harassment

Hacking

Offensive or Illegal Contents

Sextortion

Identity Theft

Cyber bullying

Cyber Stalking

Online Scams and Fraud

Phishing

### Citizens Education and Awareness

Capacity building and education is another important component of MAUCORS. It provides detailed information on the various types of cybercrimes, its preventive measures and the actions that should be taken in case citizens become victim. It also educates and guides parents with regard to child online safety. The latest news on cybercrime is also available on its news section. The portal also has a Frequently Asked Questions (FAQ) section, which addresses common concerns, questions or objections that citizens can have.

### Post Implementation of MAUCORS

The implementation of MAUCORS is a significant initiative in our fight against cybercrime. During its first four months of operation, MAUCORS is already helping to achieve these goals. With over 210 reports received, the CERT-MU and other government institutions are starting to build the much needed picture of the types of cybercrime affecting the Mauritian cyberspace. Apart from facilitating reporting of incidents, MAUCORS is helping to create a cyber-literate public. Through MAUCORS, citizens are learning how to stay safe online, how to engage in the digital economy and the need to report an incident when it occurs.

Combatting cybercrime is a challenging task due to its ever evolving nature. As a result, cybercrime poses significant challenges for law enforcement. The nature of the internet, relative anonymity, its global nature, the speed and volume of transactions, are challenges to the traditional law enforcement. Tackling cybercrime requires a coordinated effort. The establishment of MAUCORS provides a collaborative framework of different institutions to deal with the detection, investigation and prosecution of cybercrime.

**M**AUCORS is the national cybercrime online reporting system that allows citizens to securely report instances of cybercrime. It streamlines the process of incident reporting between law enforcement agencies and other relevant government agencies. Being a key initiative under the National Cybercrime Strategy to combat cybercrime, MAUCORS fosters an intelligence-led approach and better information sharing between different agencies that are working together to make Mauritius a hard target for cyber criminals. Citizens are encouraged to make utmost use of MAUCORS and reports incidents in a more effective and secure way.

### DID YOU KNOW?

**As at July 2018, Facebook is ranked as the most popular social networking site and is the first social network to surpass 1 billion registered accounts. It currently sits at 2.2 billion monthly active users.**

**The Sixth-ranked photo-sharing app Instagram had 1 billion monthly active accounts.**

# The General Data Protection Regulation (GDPR) from an IT Security Perspective

Personal data protection plays an important role in the digital era of Mauritius. The need of having a data protection law is derived from the principle that everyone has the right to protect their private life, of which personal data forms an integral part. The right to privacy is expressly provided in Sections 3 and 9 of the Constitution of Mauritius and Article 22 of the Mauritian Civil Code. In 2004, Mauritius enacted the Data Protection Act 2004, which provided for the protection of the privacy rights of individuals in view of the developments in the techniques used to capture, transmit, manipulate, record or store data relating to individuals.

In light of the digital evolution in Mauritius, the Data Protection Act 2004 has been replaced by the Data Protection Act 2017 (DPA 2017), which came into force on 15 January 2018. The Act aims at strengthening the control and personal autonomy of data subjects over their personal data and for matters related thereto. It seeks to bring Mauritius data protection framework into line with the General Data Protection Regulation (Regulation (EU) 2016/679).

The GDPR is a regulation that requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The European Parliament adopted the GDPR in April 2016, replacing an outdated data protection directive from 1995. It carries provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. The GDPR also regulates the exportation of personal data outside the EU. To harmonise data privacy laws, the GDPR provisions are consistent across all 28 EU member states. GDPR came into existence due to public concern over privacy. The GDPR replaces and addresses the loopholes in the 1995 EU Data Protection Directive.

The Data Protection Act 2017 of Mauritius has been aligned with the GDPR and came into effect in January 2018. The Act aims at strengthening the control and personal autonomy of data subjects over their personal data and for matters related thereto. It also brings the Mauritius data protection framework in line with international standards. The GDPR intends to strengthen and unify data protection for all individuals within the EU and addresses the export of personal data outside the EU. It provides for a harmonisation of the data protection regulations throughout the EU, thus making it easier for non-European companies to comply with these regulations.

The alignment of the Data Protection Act with the GDPR has several benefits. Firstly, the GDPR has cross-border capability, which means that:

⇒ the GDPR will apply to every data controller/ processor1, regardless of location, that processes EU citizens' and residents' personal data;

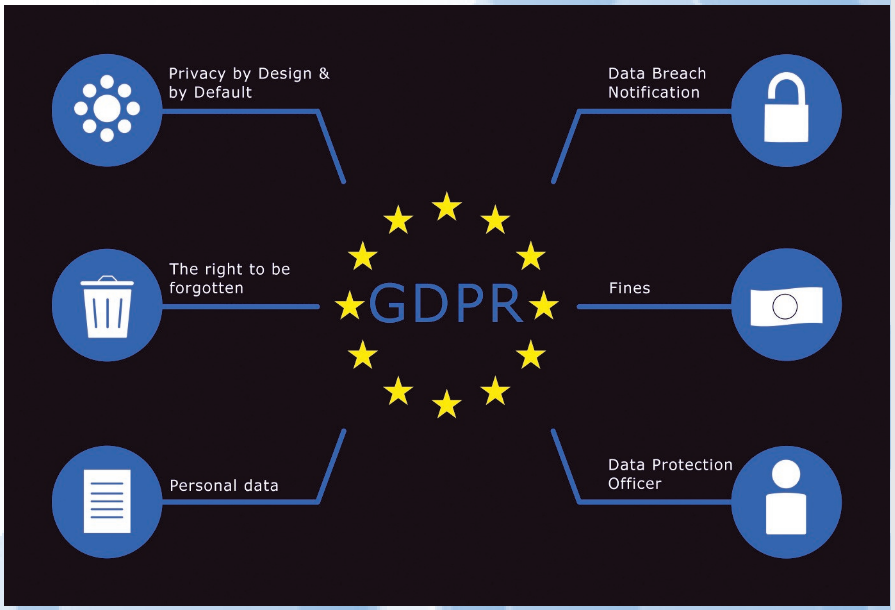
⇒

⇒ the GDPR will apply if the data controller, processor or subject is based in the EU; and

⇒ EU citizens' personal data will not be transferable to a country that does not have similar regulations as the GDPR.

For example, GDPR will not only apply to an EU based company wants to collect personal data of a Mauritian citizen/employee , but also will apply to a Mauritian company wanting to collect data about an EU citizen/employee. Thus, the collection of information (both ways) will be possible only if Mauritius has the Data Protection Law which are similar to the EU country (GDPR).

Another benefit of the GDPR is that it will help Mauritius to attract foreign investment through the facilitation of businesses working with European countries to transfer data therefrom. The Act enhances the 'ease of doing business' requirements and build trust between Europe and Mauritius. Moreover, a stronger and more coherent data protection framework, backed by effective enforcement will allow the digital economy to flourish by putting individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities. Hence, the risks of data breaches will be minimised.



**GDPR from the IT Security Perspective**

GDPR is the biggest shake-up in privacy legislation and data management approach for many years. It will have an impact on any organisation that processes personal data. Organisations that breach the regulation would be applicable to a fine up to 4% of their annual global turnover or 20 million Euros, whichever is greater. Breaches will apply to firms that do not have adequate customer consent for processing their personal data or violate the principle of the privacy-by-design concepts and model. It is important to note that both data controllers and processors are subject to the rules, especially if they fail to either carry out a privacy impact assessment or notify the concerned authority about a breach. In this article, we will look at GDPR from the IT security perspective where ISO 27001 plays an important role.

Firstly, it is important to discuss about the main characteristics of the GDPR and the key differences from the EU directives, which are listed below:

### 1. Scope

GDPR defines how EU citizens' data must be handled by countries inside and outside the EU. Furthermore, the regulations will apply to the processing of personal data in the EU by a data controller or processor who is not in the EU. For example, any business that provides services or goods to EU residents is by definition processing EU citizens' data and therefore will have to comply. In addition, GDPR encompasses personally identifiable data within social media, photos, email addresses and IP addresses.

### 2. Consent

GDPR has changed and reinforced the conditions of consent in that it expects clear, plain language consent from data subjects in an easy, accessible and intelligible form. Subsequent withdrawal of the consent must be as effortless as giving it.

### 3. Fines and Penalties

GDPR sanctions substantial fines of up to €20m or four percent of annual revenue.

### 4. Privacy by Design

Processes will need to be amended to consider privacy by design whereby the controller must apply adequate technical and organisational procedures to fulfill the requirements of GDPR and protect the rights of individuals.

### 5.Data Portability

Personally identifiable data must be portable by open use of common file formats that are machine-readable when the data subject receives them.

### 6. Right to Access

GDPR provides the right to data subjects to request the data controller to confirm whether their personally identifiable data is being processed, where, and for what purpose. In addition to this, the data controller must provide a free electronic copy of any personally identifiable data.

### 7. Right to be Forgotten

The data subject is entitled to request that the data controller permanently or on-demand delete his/her personally identifiable data, cease further distribution of the data, and demand third parties halt processing of the data.

### 8. Breach Notification

As a data breach is likely to result in a risk to the rights and freedoms of individuals, GDPR requires a mandatory breach notification to be submitted to the relevant authority within 72 hours of the organisation first becoming aware of the breach. In addition, data processors are required to notify their customers without unnecessary delay.

### 9. Data Protection Officer (DPO)

It will be mandatory for data controllers and processors to appoint a DPO. However, this only applies to those data controllers and processors whose central activities entail processing operations that need consistent and systematic monitoring of data subjects on a large scale or of special groups of data.

### Mapping IT Security Governance and GDPR

IT Governance will be impacted by the requirements of the GDPR and will bring benefits also. The regulations will encourage organisations to have a more secure data management approach in place. Compliance will require an IT governance framework to be adjusted to encompass issues such as personal responsibilities relating to data transfer, data subject consent, and privacy by design. From an IT governance perspective, organisations should focus on the dynamics of legal, technical and organisational factors.

GDPR introduces several privacy arrangements and control mechanisms that are intended to safeguard personal identifiable data. Many of those controls are also recommended by the ISO 27000 series of standards including ISO 27001:2013, ISO 27002:2013 as well as the COBIT 5 standards. For example, ISO 27001 controls such as A.18.1.4 (Privacy and Protection of Personally Identifiable Information) and A.9.1.1 (Access Control Policy) relate to privacy data transfer, data subject consent, and privacy by design. From an IT governance perspective, organisations should focus on the dynamics of legal, technical and organisational factors.

GDPR introduces several privacy arrangements and control mechanisms that are intended to safeguard personal identifiable data. Many of those controls are also recommended by the ISO 27000 series of standards including ISO 27001:2013, ISO 27002:2013 as well as the COBIT 5 standards. For example, ISO 27001 controls such as A.18.1.4 (Privacy and Protection of Personally Identifiable Information) and A.9.1.1 (Access Control Policy) relate to privacy and risk assessment. Both controls can be interpreted as addressing privacy concerns around data transfer or privacy by design in relation to personally identifiable information or data subject information.

Regarding COBIT, the IT Management Framework and its management practices of APO01 relate to organisational structure. COBIT 5 also refers to privacy officers with responsibility for screening the risk and organisational impacts of privacy regulations while ensuring such legislations are adhered to. This definition is similar to article 37 of GDPR with its requirement for the designation of a Data Protection Officer (DPO).

As discussed, the aspects of GDPR that directly concern IT security governance are varied. One of the main issues, however, will be to assess the capability of IT governance to identify and pinpoint identifiable personal data in the organisation. This is a condition of Article 30, regarding requesting records of processing activities.

In addition, it is a requirement for rights of access by the data subject in Article 15, the modification of incorrect personal data in Article 16, and the right to be forgotten in Article 17. Therefore, these requirements provide a good basis for readiness. Organisations with good data management in place that enable them to describe the information lifecycle will automatically be compliant with most of the GDPR requirements.

To work towards ensuring compliance of their data, organisations should therefore take the following actions:

⇒ Establish and locate all personal identifiable data that is within the scope of GDPR.
⇒ Focus explicitly on data risk management for a complete risk picture of data, using data categorisation based on their processing and storage in various services and facilities.
⇒ Note that an effective data risk management demands a definition of adequate protection process and procedures for the various categories of GDPR data.
⇒ Coordinate and map data protection needs to other services and IT systems across the entire organisation.

It is evident that the GDPR provides enhanced safeguarding of personal data and give data subjects more control over their data. With a comprehensive plan in place, organisations that act as data controllers or processors will be able to ensure compliance with the new rules in a timely manner, including implementing an adequate testing period. Organisations will need to investigate their current IT security and data protection practices to perform a gap analysis between where they are now and where they need to be with the GDPR. Adopting recognised standards such as ISO27001 will go a long way towards achieving greater transparency over data, and building regular reviews into such activities will also support compliance going forward. Robust tried and tested controls will support IT governance activities and protect individuals from loss of control over their personal data, as well as businesses from financial and, not to be underestimated, reputation loss through failure to comply with the new regulations.

## 3 Emerging Innovations in Technology that Will Impact Cyber Security

### Hardware Authentication

It is a well-known fact that passwords and usernames used by a majority of data users are weak. This makes it easy for hackers to get access to the information systems and compromise sensitive data of a business entity or government agency. In turn, this has exerted pressure on experts of systems security to come up with authentication methods that are more secure. One of the ways that has been used is the development of user hardware authentication. Tech gurus have developed a solution in the user authentication process with a new Core vPro processor that belongs to the sixth generation of processors. The core vPro can combine different hardware components with enhanced factors simultaneously for user identity validation purposes.

The tech company Intel has built on previous experiences and mistakes and dedicated a portion of the processor for security reasons to make a device part of the entire process of authentication. Hardware authentication can be especially important when it comes to the Internet of Things (IoT) where the network of connected devices ensures that any device that seeks to be connected has the rights for connectivity to that particular network.

### Cloud Technology

The cloud is set to have a significant impact on the transformation of systems security technology. More business enterprises and government agencies have embraced cloud technology to store the vast amounts of information that they generate on a daily basis. There will be more approaches to information systems security that will be developed for use in the cloud. Techniques for on-premise data storage will be migrated to the cloud. Components such as virtualized intrusion detection and prevention systems, virtualized firewalls and virtualized systems security will now be used from the cloud as opposed to the traditional forms.

### Deep Learning

Some technologies are encompassed in deep learning, such as machine learning and artificial intelligence. There is a significant deal of interest for purposes of systems security in these technologies. Deep learning, just like behavior analytics, focuses on anomalous behaviour. Whenever AI and machine learning systems are fed with the right data regarding potential systems security threats, they can make decisions on how to prevent hacks depending on their immediate environment without any human input.

The system scrutinizes entities instead of users that have access to the information system. The most recent developments in machine learning technology and exact business analytics means that we can now be able to analyze the different entities that are found in the enterprise at both the macro and the micro levels. Business organizations and government agencies can now be able to stamp out any persistent or advanced cyber threats using artificial intelligence and machine learning.

# News Focus

## Patch August 2018: Microsoft corrects two actively exploited zero-day

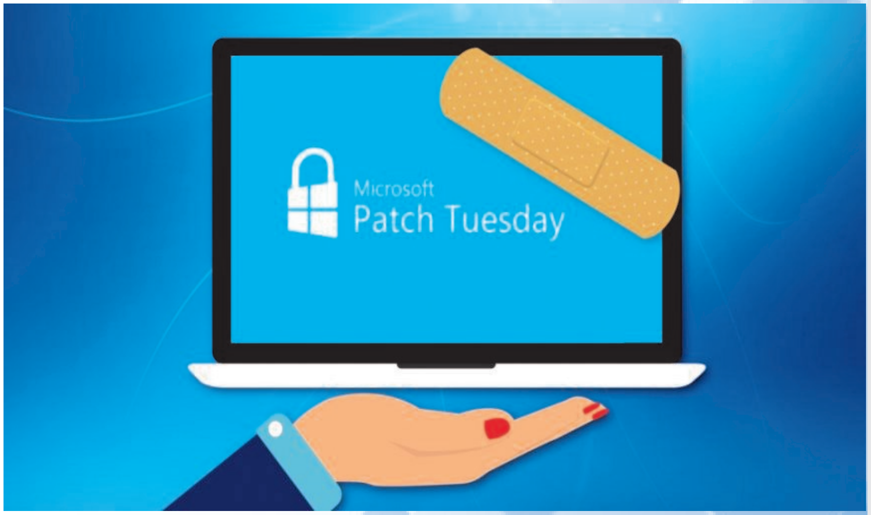
Microsoft Corporation released a series of patch as part of the August 2018 updates which addressed 60 flaws, two of which have been reportedly been actively exploited as zero-days. Collectively, the repairs address bugs found in Internet Explorer, Microsoft Edge, Windows, Microsoft Office (and Office Services and Web Apps), ChakraCore, Adobe Flash Player, .NET Framework, Microsoft Exchange Server, Microsoft SQL Server, and Visual Studio.

The first exploited flaw is CVE-2018-8373, a critical memory corruption vulnerability in Internet Explorer's scripting engine. According to a Microsoft advisory, attackers can exploit the bug to execute arbitrary code and gain the same rights as the current user. If that user has admin privileges, then the attackers could hijack the affected system and subsequently install programs, view or alter data, or create new accounts with full user rights.

In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Internet Explorer and then convince a user to view the website," the advisory states. An attacker could also embed an ActiveX control marked 'safe for initialization' in an application or Microsoft Office document that hosts the IE rendering engine. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.

Trend Micro researcher Elliot Cao, who reported CVE-2018-8373 in conjunction with his company's Zero Day Initiative, said that the issue is similar to another actively exploited vulnerability that was patched last May in Microsoft's VBScript engine, Trend Micro revealed via its own blog post. In other words, if there are similar bugs to this one, they will likely be found and exploited, too, the post asserts.

The other exploited bug, CVE-2018-8414, was designated merely as important, despite allowing remote code execution when the Windows Shell fails to properly validate file paths. Attackers who capitalize on this flaw by tricking users into opening a specially crafted file (via email or compromised/malicious website) can take control of an affected system if said user is logged on as an administrator, another Microsoft advisory warns.



Microsoft has credited Matt Nelson of SpecterOps with uncovering the exploited RCE bug.
Microsoft also issued three separate security advisories, two of which address newly discovered speculative execution side-channel attack vulnerabilities in the same vein of well-known vulnerabilities Spectre and Meltdown.

As part of their own coverage of August Patch, McAfee stated that it reported an elevation of privilege vulnerability (CVE-2018-8253) in the Windows Cortana virtual assistant, while Okta announced its discovery of a security feature bypass vulnerability (CVE-2018-8340) in the Active Directory Federation Services (ADFS) protocol that can allow attackers to subvert certain multi-factor authentication factors.

Users are advised to watch out for the vulnerabilities and apply the workarounds accordingly.

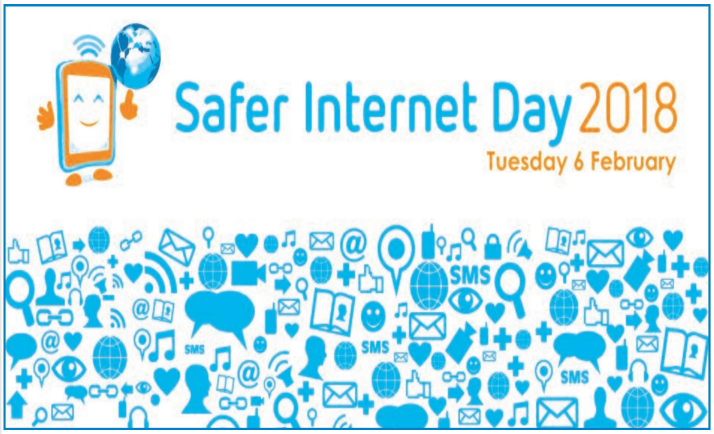
**Security Tip:**

**Keep your system up-to-date by applying regular patches and updates from vendors.**

# CERT-MU Events

## Safer Internet Day

Safer Internet Day is part of a global drive to promote a safer Internet for all users, especially for young people and is celebrated worldwide on every second Tuesday of February each year. On this occasion, the Computer Emergency Response Team of Mauritius (CERT-MU), organised the SID on Tuesday 6th February 2018 at Sir Abdool Raman Osman State College in collaboration with the Ministry of Education & Scientific Research. The theme for this year is *"Create, Connect & Share Respect: A Better Internet Starts with You"*. The objective of SID is to promote safer and more responsible use of online technology and mobile phones, especially amongst children and young people



## Launching of MAUCORS and Cyber Security Drill for Top Management

The Computer Emergency Response Team of Mauritius (CERT-MU) organised the launching ceremony for the Mauritian Cybercrime Online Reporting System (MAUCORS) and a Cyber Drill for Top Management in collaboration with the International Telecommunication Union (ITU) at Le Meridien Hotel on Thursday 15th March 2018. The Mauritian Cybercrime Online Reporting System (MAUCORS) was officially launched by the Honourable Yogida Sawmynaden, Minister of Technology, Communication & Innovation. This system will help to coordinate and resolve social media incidents efficiently. This system has been developed by the CERT-MU and is one of the key initiative under the newly drafted Cybercrime Strategy that sets out the Government's approach to combat cybercrime in Mauritius. The cyber drill for top management was also officially opened on the same day. Professor Dr. Marco Gercke, representative of the International Telecommunication Union (ITU) conducted the cyber drill for top management of organisations. The objective of this drill was to demonstrate the top executives to assess organizations' preparedness to resist cyber threats and enable timely detection, response, and mitigation and recovery actions in the event of cyber-attacks. The launching ceremony was attended by around 70 participants and the cyber drill was attended by 55 participants.

## Training on Cyber Defense Monitoring and Forensics

The Computer Emergency Response Team of Mauritius (CERT-MU) in collaboration with the Command and Control Centre of Kenya organised a 3-day training programme on Cyber Defense Monitoring and Forensics at Voilà Hotel, Bagatelle from the 27$^{th}$ February – 1$^{st}$ March 2018. The training course provided an introduction to Network Security Monitoring (NSM), Security Information and Events Management (SIEM), Malware Analysis and Digital Forensics. Major part of the course was hands-on case studies and analysis exercises using real world data. The main focus of the training programme was on intensive hands-on sessions on addressing key challenges faced by local organizations in all sectors/industries. A wide range of commercial and open source tools were used to equip cyber defenders with the necessary skills to anticipate, detect, respond and contain adversaries. The training programme was followed by 23 participants from the public and private sector.

# Information Security Tips

Be conscientious of what you plug in to your computer. Malware can be spread through infected flash drives, external hard drives, and even smartphones.

Back up your data regularly, and make sure your anti-virus software is always up to date

Always be careful when clicking on attachments or links in email. If it's unexpected or suspicious for any reason, do not click on it.

Make sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, it could be a sign that you have been compromised.

Never leave your devices unattended. If you need to leave your computer, phone, or tablet, lock it up so no one can use it while you are out. If you keep sensitive information on a flash drive or external hard drive, make sure to lock it up as well.

## Computer Emergency Response Team of Mauritius (CERT-MU)

National Computer Board
7th Floor, Stratton Court,
La Poudriere Street, Port Louis

Tel: 210 5520
Fax: 208 0119

**Website: www.cert-mu.org.mu**

**Incident Reporting**
Hotline: 800 2378
Email: incident@cert.ncb.mu

**Vulnerability Reporting**
Email: vulnerability@cert.ncb.mu

**For Queries**
Email: contact@cert.ncb.mu