MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

ADDRESSING CYBER SECURITY MEASURES

Distinguished Professor Dato' Dr. Rajah Rasiah
University of Malaya

Dr. Maslina Daud CISSP CISM
CyberSecurity Malaysia

12th October 2022

CYBER SECURITY INCIDENTS

CyberSecurity MALAYSIA

European Car Plants Halted by WannaCry Ransomware Attack

France's Renault and its Japanese alliance partner Nissan have been forced to temporarily i some of their plants in Europe.

KIM ZETTER SECURITY MAR 3, 2016 7:00 AM

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere.

The New York Times

Meat processor JBS paid $11 million in ransom to hackers.

The breach was the latest in a string of attacks targeting businesses critical to American infrastructure.

AEROSPACE AND DEFENSE MAY 25, 2016 / 5:15 PM / UPDATED 6 YEARS AGO

Austria's FACC, hit by cyber fraud, fires CEO

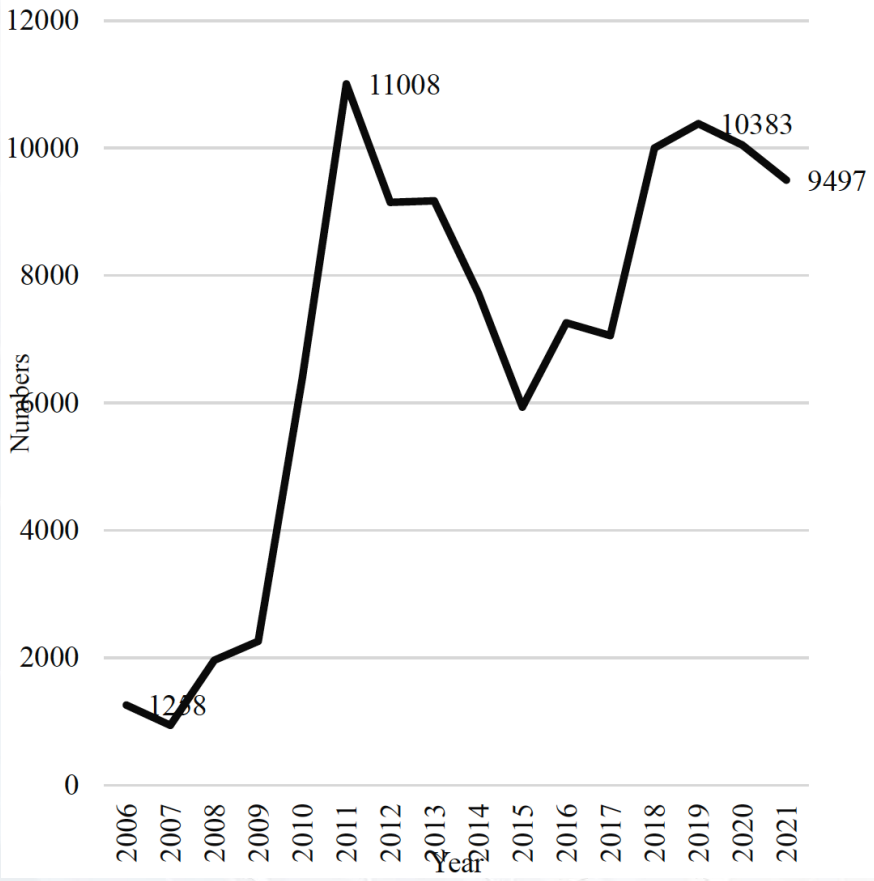
By Reuters Staff

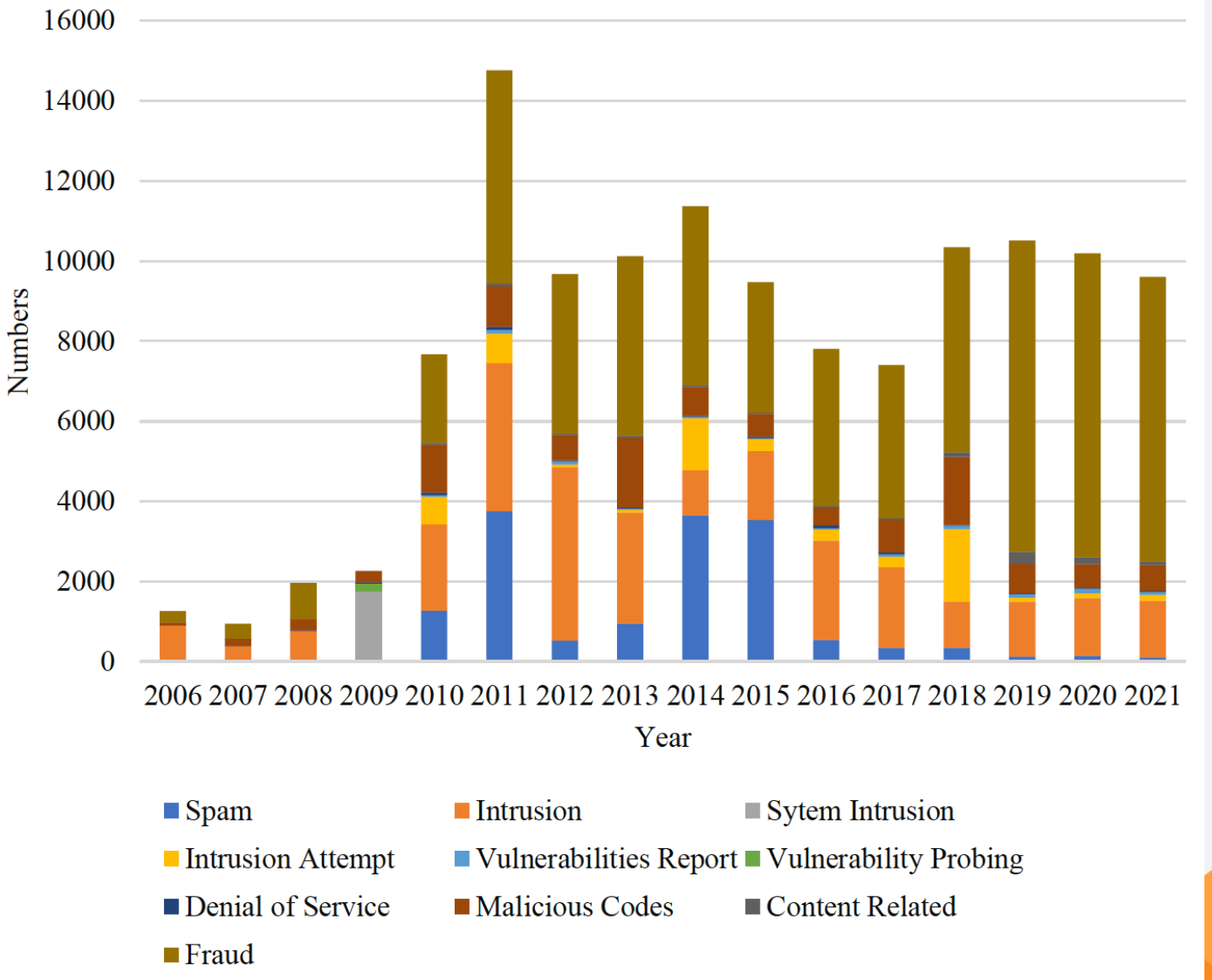
2 MIN READ

VIENNA (Reuters) - The head of Austrian aerospace parts maker FACC has been fired after the company was hit by a cyber fraud that cost it 42 million euros ($47 million).

Record-breaking DDoS reportedly delivered by >145k hacked cameras

CYBER SECURITY INCIDENTS IN MALAYSIA



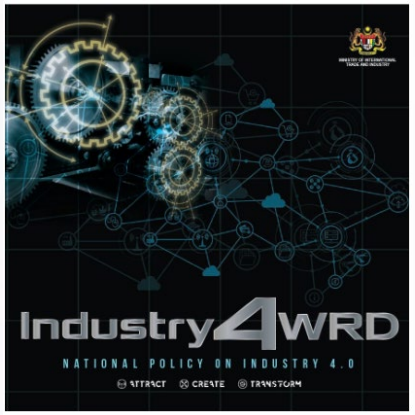


(Source: Plotted using data downloaded from MyCert (2022)

NATIONAL POLICIES

- Thrust 6 focuses on cyber security that aims to create a trusted, secure and ethical digital environment
- Four strategies were formulated under this thrust:
  - strengthening safety and ethics in digital activities
  - enhancing institutions' commitment to data protection and privacy
  - cross-border data transfer improvements
  - increasing cyber security uptake among businesses.

- Emphasizes the legal framework that governs personal data management and cyber security to boost trust in online activities
- Enhance sMalaysia's existing cyber security framework by incorporating safeguard measures for the smooth implementation and operationalisation of technologies



- Requires improvements in data integrity, security standards and compliance
- Provides a seamless integration platform and coordination between different actors in manufacturing value chains

- Provides strategies and tools in providing trust in cyber security environment
- Supports government agenda in the national initiatives, Industry 4 and adoption of disruptive technologies

TECHNOLOGY DOMAINS IN IR4.0

- Internet of Things
  - IoT for consumer's convenience, IIoT for industrial operations
  - Prevalence of IoT devices demands increased interconnectivities, but ill-equipped with security features eg. authentication, encryption
  - General features - limited memory and processing power
  - Users' security awareness is crucial eg change default password
  - Open up for large and complex attack surface eg MIRAI attack

- Artificial Intelligence
  - Able to address cybersecurity threats (eg intrusion detection), but also introduces security vulnerabilities when AI attacks its own system
  - Two main assets:
    - Big data collected to learn and train for prediction
    - Data model arising from the AI training
  - Security attacks include; data alteration, dataset poisoning, algorithm poisoning, model poisoning

TECHNOLOGY DOMAINS IN IR4.0

- Robotics process automation
  - Improves efficiency with less involvement of human
  - Misconfigurations of the automated process pose security risks
  - Use of robotic controlled by AI modules pose security threats when AI modules are compromised
- Big Data Analytics
  - Its characteristics-variety of data, velocity, volatility, value introduce security risks
  - Data variety leads complexity in data management
  - Data volatility creates challenges to keep and manage audit trail
  - Data segregation is a challenge to determine protection measures
  - Affect system performance especially during encryption

MANUFACTURING SECTOR IN IR4.0

- Convergence of Information Technology and Operational Technology
- OT comprises components eg PLC, RTU that are designed with no security in mind and are legacy systems
- IIoT devices bridge the industrial operations and corporate network together with RPA and AI
- Increasing connectivity increase security risks due to inherent vulnerabilities of the OT systems
- Integration of legacy systems with advanced systems due requirement for shifting from mass production to mass customization introduce new risks and vulnerabilities
- Using RPA without proper configuration can elevate further risks

"Known vulnerabilities related to industrial control systems (ICS)—and, by extension, operational technology (OT)—as well as Internet of Things (IoT) vulnerabilities are increasing each year, with an appreciable increase in identified vulnerabilities from 2020 to 2021"

Source: https://www.ibm.com/downloads/cas/ADLMYLAZ

AGRICULTURE SECTOR IN IR4.0

- Precision agriculture use data collected by GPS, IoT Satellite imagery
- Data collection and monitoring is very specific to geographical location, weather, climate
- Security threats - IP theft and disruption of food production
- Lack of skilled workers to interpret and make use of the data, but also in cybersecurity
- To design farming equipment taking into account cybersecurity considerations

SERVICES SECTOR IN IR4.0

- E-commerce involving PII and credit cards where large pool of data transmitted

- Concerns grow on cross border data
  - use of cloud computing platform that create challenges for some jurisdictions

- Exchange of product and personal data requires a trusted platform through assurance of security measures

OTHER CYBERSECURITY CONCERNS

- Transition to 5G
  - Offers a large and complex attack surface due to Increased connectivity and speed with low latency

- Legacy system
  - Inherent vulnerabilities
  - Challenges on preservation of information security due to integration with advanced technologies eg IoT, AI

18/09/2022, 19:00 FBI Warns of Cyberthreats to Legacy Medical Devices

Data Breach Today
Prevention. Response. Notification.

https://www.databreachtoday.com/

Governance & Risk Management , Healthcare , Industry Specific

FBI Warns of Cyberthreats to Legacy Medical Devices

Bureau Is Latest Federal Agency to Address Long-Standing, Growing Problem

Marianne Kolbasuk McGee (HealthInfoSec) • September 14, 2022

The FBI is the latest federal agency warning of cyberthreats facing legacy medical devices.

The FBI is the latest federal agency warning healthcare sector entities of cyberattack threats to medical devices, especially unpatched and outdated products, recommending that organizations take steps to identify vulnerabilities and "actively secure" the gear.

SECURE BY DESIGN

- Focuses on building security controls into a product's design and from the basic building to the entire IT design
- An approach to strengthen cybersecurity while reducing the likelihood of cybersecurity breaches through measures such as:
  - ✓ continuous testing
  - ✓ authentication safeguards
  - ✓ adherence to best programming practices
- All security controls should be designed with the core pillars of information security in mind - C,I,A
- Security requirements for systems development should be embedded as part of the procurement process as this provides a more cost-effective approach
- Preventing rather than fixing security issues is less costly!

STRUCTURED SECURITY PROCESSES

PROACTIVE

- Information security Management System- a risk-based approach
- Business Continuity Management- availability of information to avoid services disruption and increase business resilient
- Vulnerability assessment and penetration testing- to identify vulnerabilities before being exploited
- Source code review

RESPONSIVE

- Incident management- to manage security event before it becomes a crisis
- Digital forensic- to identify source of security events that leads to security incidents

SECURITY ASSURANCE

- Devices and products eg IoT, medical devices
  - Security features to be embedded from the design process by manufacturers and developers
  - Security evaluation and testing
  - ISO/IEC 15408 Common Criteria for security product certification
- Process
  - ISMS (ISO/IEC 27001)
  - Cloud security (ISO/IEC 27017) extension to ISO 27001
- Platforms
  - Trusted websites – for e-commerce or any other services
  - Cloud – Paas environment
- People
  - Skillsets and certification eg ISC2, ISACA,SANS

SKILLED WORKERS, TALENTS AND AWARENESS

- Urgent needs to have talented and skilled workers with diverse skillsets in critical industries that are adopt advanced technologies
- Relevant programmes to be established for new skills, up-skilling and re-skilling
- Staff turnover can be a threat to organisations
- Security awareness for all stakeholders

SECURITY GOVERNANCE

- The needs for a centralised platform with regulatory role to govern and monitor security initiatives effectively
- Regulatory role is crucial to ensure secure devices, platform and environment are used within the ecosystem for a safe and secure computing
- To effectively govern information exchange and operations

CONCLUSION

- The government and intermediary organisations to play an important role for all stakeholders to serve their intended purposes
- Various technologies of IR4.0 require security measures and strategies on the massive data produced
- Cooperation among all national cybersecurity organizations to strengthen protection and privacy of users and producers
- Workforce in the cybersecurity domain is a very serious matter
- Security shall not be an afterthought

MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

THANK YOU

Corporate Office
CyberSecurity Malaysia
Level 7, Tower 1, Menara Cyber Axis
Jalan Impact, 63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

T +603 8800 7999 | **F** +603 8008 7000 | **H** +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

www.facebook.com/CyberSecurityMalaysia
CyberSecurity Malaysia
twitter.com/cybersecuritymy
cybersecurity_my
www.youtube.com/cybersecuritymy

JUBLI PERAK 1997 - 2022 CyberSecurity MALAYSIA

KITA SIBER
HARI KESELAMATAN INTERNET 2022: EDISI MALAYSIA

Best Brand Internet Security 2008 & 2009

CERTIFIED TO ISO/IEC 27001:2013
CERT. NO. : ISMS 00114

ACB ISMS 02
SAMM 456

Status Company

WSIS PRIZES 2020 WINNER www.wsis.org

THE MALAYSIA BOOK of RECORDS