Cyber Resilience Capacity Building

Workshop 1: Introduction to Organizational Cyber Resilience Management

Tuesday, 1st December 2020

A COLLABORATION BETWEEN:

WITH SUPPORT FROM:
<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>09h40</td>
<td>Arrival and Registration</td>
</tr>
<tr>
<td>09h55</td>
<td>Preliminaries:</td>
</tr>
<tr>
<td></td>
<td>- Overview and housekeeping by <strong>Christy Un</strong> <em>(UNU)</em></td>
</tr>
<tr>
<td></td>
<td>- Welcome by <strong>Jingbo Huang</strong> <em>(UNU)</em></td>
</tr>
<tr>
<td></td>
<td>- Workshop overview by <strong>Mamello Thinyane</strong> <em>(UNU)</em></td>
</tr>
<tr>
<td>10h10</td>
<td>Session 1: ICT Management in Organizations (25 mins) by <strong>Farzad Sabetzadeh</strong> <em>(Faculty of Business – CityU Macau)</em></td>
</tr>
<tr>
<td>10h35</td>
<td>Session 2: Organizational Risk Management (50 mins) by <strong>Tiffany Leung</strong> <em>(Faculty of Business – CityU Macau)</em></td>
</tr>
<tr>
<td>11h25</td>
<td>Break</td>
</tr>
<tr>
<td>11h35</td>
<td>Session 3: Cybersecurity Risk Management (55 mins) by</td>
</tr>
<tr>
<td></td>
<td>- <strong>Mamello Thinyane</strong> <em>(United Nations University)</em></td>
</tr>
<tr>
<td></td>
<td>- <strong>Terry Cheung</strong> <em>(TopSOC)</em></td>
</tr>
<tr>
<td></td>
<td>- <strong>Debora Christine</strong> <em>(United Nations University)</em></td>
</tr>
<tr>
<td>12h30</td>
<td>Session 4: Local Cybersecurity Landscape (30 mins) by <strong>Emil Marques</strong> <em>(Faculty of Business and Law - USJ)</em></td>
</tr>
<tr>
<td>13h00</td>
<td>Closing</td>
</tr>
</tbody>
</table>
Welcome

Jingbo Huang
Workshop Overview
Mamello Thinyane
HEALTH BUREAU’S ONLINE SYSTEM FALLS VICTIM TO CYBERATTACK

LYNY VALLES  WEDNESDAY, JANUARY 29, 2020 - 7 MONTHS AGO  NO COMMENTS

The online system of the Health Services Bureau (SSM) suffered from a DDoS (Distributed Denial of Service) attack on Tuesday, disrupting the network service of the health declaration system and...

ANIMA VICTIM TO THIRD CYBER ATTACK IN TWO MONTHS

LYNY VALLES  FRIDAY, JANUARY 16, 2016 - 3 YEARS AGO  1 COMMENT

Local animal rights group Anima (Macau) said it was this week victim to the third cyber attack in two months, suspecting that the Macau Vet...

NEW MACAU FACES CYBERATTACKS, THREATS DUE TO VOTING ACTIVITY

LYNY VALLES  MONDAY, AUGUST 14, 2016 - 1 YEAR AGO  NO COMMENTS

Local pro-democracy group New Macau Association (ANJM) said that the website where it has been conducting its voting activities on universal suffrage has been subject to cyberattacks and that...

PORTUGUESE SCHOOL IT SYSTEM HACKED FOR RANSOM

LYNY VALLES  FRIDAY, AUGUST 14, 2015 - 2 MONTHS AGO  NO COMMENTS

The former head of the Macau Management of the Education Department (DSE) was the target of a ransomware attack this week, according to several local sources.

PUBLIC SECTOR LAGS BEHIND PRIVATE IN INFORMATION SECURITY

LYNY VALLES  FRIDAY, JANUARY 15, 2016 - 3 YEARS AGO  NO COMMENTS

According to the results of the “Macau Information Security Survey 2015” conducted by the Macau New Technologies Incubator Center (MSTIC), the government sector continues to lag behind the private sector...

MARRIOTT SECURITY BREACH EXPOSE DATA OF UP TO 500M GUESTS

LYNY VALLES  FRIDAY, OCTOBER 30, 2015 - 2 YEARS AGO  NO COMMENTS

Hackers stole information on as many as 500 Marriott hotel guests over four years, obtain passport numbers and other personal information...

CYBERSECURITY LAW ENTERS INTO FORCE, P. LAUNCHES CAR

LYNY VALLES  TUESDAY, DECEMBER 31, 2014 - 4 MONTHS AGO  80 COMMENTS

To cope with their new duties under the Cybersecurity Law, officers have been taking a course to get their game props and code for game props...
Impact of Adverse Cyber Events

**Direct costs**
- Financial losses
- Data losses
- Remediation

**Indirect costs**
- Reputation
- Client trust
- Opportunity costs
- Productivity

Average annual cost of cybersecurity incident for SMEs USD34,606... (for large organizations USD30 million)
Cyber Resilience for organizations

The ability for organizations to continue functioning (i.e., meeting objectives, maintaining operations, providing services to clients) despite significant adverse cyber incidents (e.g., cyber attacks, environmental threats)
Cyber Resilience phases

1. PREPARE
   - Awareness-raising
   - Capacity-building
   - Redundancy measures
   - Recovery plan
   - Logging and monitoring
   - Prevention measures
   - Active mediation
   - Web hygiene
   - Attitudinal measures
   ... 

2. ABSORB
   - Alternative resources
   - Withstand measures
   - Incident reporting
   - Threat removal measures
   - Sandboxing and isolation
   - Engage measures

3. RECOVER
   - System recovery
   - Account recover
   - Data recovery
   - Professional support
   - Social support

4. ADAPT
   - Evolve measures
   - System upgrades
   - Resource swapout
   - Bounce forward
   - Enhanced capacity
Cyber Resilience Capacity Building

- Introduction to Organizational Cyber Resilience Management
- Everyday Cybersecurity in Organizations
- Introduction to Cybersecurity Support in Organizations
Session 1: ICT Management in Organizations

Trainer: Farzad Sabetzadeh
Assistant Professor
Faculty of Business
Some Questions to Start With…

Why is it that Information Technology (IT) can be an organization’s strategic enabler and differentiator—or can cripple an organization—yet IT remains under-resourced in NGOs?

Why is there a global shortage of qualified cybersecurity professionals and why do organizations struggle to employ them?

What alternatives do organizations have with regards to IT deployment?
Organizational Value Creation

**People**
- Personnel who interact in organizations processes and contribute to services and value creation

**Processes**
- Goal and mission-oriented activities conducted by an organization

**Technology**
- Information and communication technologies used to facilitate and support organizations activities

**Partners**
- External organizations that support and contribute to an organizations processes and value creation
Why Organizations Use IT?

- Operational efficiency
  - And improving productivity

- Engagement with clients and partners
  - Easy interaction and communication with clients

- Competitive advantage
  - Improved relative performance of the organization

- New product, services, and business models
  - Providing new times of services to client

- Improved decision-making
  - Data analysis, forecasting

- Survival
  - Cost savings
  - Compliance with rules and regulations
Types of IT Systems Used in Organizations

Transaction Processing Systems
- For processing of organizational transactions

Office Automation Systems
- Support office activities including word processing, calendar and events, communication

Decision Support Systems
- Systems that support decision making by top-managers - analysis, forecasting

Knowledge Management Systems
- Support the creation and sharing of knowledge within an organization

Management Information Systems
- Systems that support planning, controlling and decision by middle management

Executive Support Systems
- Information systems that support decision-making at the top-level of an organization

Others
- Customer Relationship Management Systems (CRMS), Business Intelligence Systems (BIS)
(Common) IT Roles and Responsibilities

IT Manager
- Governance and strategic management of the organization’s overall technology
- Includes: Chief Information Officers, Chief Technical Officer, ...

System Administrator
- Managing and maintaining organizations IT infrastructure and systems
- Includes: network administrator, ...

Support Technician
- Maintaining operational technologies and applications and assisting with the use of IT to all areas of the organization
- Includes: hardware technician, help desk support, ...

Depends on the organization’s
Thinking about CHANGE in Organizations

Change is a risky activity – many organizational changes fail or do not realize their intended outcomes. This raises the question: why is change so prevalent?

Pressure to change comes from:
- External, environmental pressures
- Internal, organizational pressures

Pressure to change

$\text{Pressure to change}$
ICT Cost vs. Innovation For Cyber Resilience

Choose the right Benchmark

Allocate resources

Keep It Simple and Secure (KISS principle)
IT Deployment Options

In-house (on-premise) deployment
- E.g., own NAS (Network Attached Storage)

Cloud services
- E.g., cloud storage such as Dropbox, Macau Drive

Hybrid
- Combination of in-house and cloud deployment
In-house (on-premise) IT Deployment

In-house deployment is a model where the IT infrastructure is housed at the organization’s premises and managed by the organization.
In-house IT Deployment Benefits

- High level of control
- Easier to ensure compliance
- No need to rely on Internet
- Can be cost-effective for small-to-mid sized organizations
- Keep critical data in-house
In-house IT Deployment Challenges

Needs physical space and resources

Cost of managing and maintaining IT
- Operations
- Licenses
- Potential risks

No guarantees
Cloud computing is a model for enabling convenient, on-demand network access to configurable computing resources (e.g., servers, storage, applications, and services) with minimal management effort or service provider interaction.

~ NIST
Cloud Deployment

Benefits

1- Economic reasons.
- low infrastructure investment.
- low cost - customers are only billed for resources used.

2- Convenience and performance.
- Application developers enjoy the advantages of a just-in-time infrastructure;
- The execution time of compute-intensive and data-intensive applications can, potentially, be reduced through parallelization.
- Cloud computing is also beneficial for the providers of computing resources- it typically leads to a higher level of resource utilization.
Challenges for Cloud Computing

Availability of service
- What happens when the service provider cannot deliver?

Diversity of services
- Data organization
- Limit user mobility
- Provider / vendor lock-in

Data confidentiality and auditability

Data transfer bottleneck
- When many applications are data-intensive.

Performance unpredictability
- One of the consequences of resource sharing.

Resource management
- Are self-organization and self-management the solution?

Security and confidentiality
What Should and Should not go into Cloud Applications

Ideal applications for cloud computing:
- Web services
- Database services
- Transaction-based service.

Applications unlikely to perform well on a cloud:
- Applications with a complex workflow and multiple dependencies,
- Applications which require intensive communication among concurrent instances (Low latency)
- Extremely secure systems
Cloud Computing and Cyber Resilience

Geographic failover capability for critical services in the time of major crisis

Scalability of services during unprecedented demand in major events/crisis
Thank You

Any Questions?
Session 2: Organizational Risk Management

Trainer: Dr. Tiffany, C. H. Leung

Assistant Professor
Faculty of Business
ERM Defined:

“... a process, effected by an entity‘s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

- Risk Management (風險管理)
- Governance (管治)
- Control (控制)
- Assurance (and Consulting) (保證(和諮詢))

Why ERM is Important

Underlying Principles:

• Every entity, whether for-profit or not-for-profit, exists to realize value for its stakeholders.

• Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

ERM supports value creation by enabling management to:

• Deal effectively with potential future events that create uncertainty.

• Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.
Stakeholders (利益相關者) are those individuals or groups that depend on an organisation to fulfil their own goals and on whom, in turn, the organisation depends.
This COSO ERM framework
• defines essential components
• suggests a common language
• provides clear direction and
• guidance for enterprise risk management.

Enterprise risk management (ERM) requires an entity to take a portfolio view of risk.

Management considers how individual risks interrelate (個人風險相互關聯).

Management develops a portfolio view from two perspectives:
• Unit level (部門層面)
• Entity level (整個組織層面)
The ERM Framework

Entity objectives can be viewed in the context of four categories:
• Strategic (戰略)
• Operations (運作方式)
• Reporting (報告)
• Compliance (合規)

The 8 components are interrelated (相關)
The ERM Lifecycle

1. Culture
2. Goal Setting
3. Identify and prioritize risks
4. Evaluate options
5. Confirm next steps
6. Implement
7. Evaluate Performance

Culture 目標設定 事件識別 風險評估 風險應對 控制活動 信息通訊 監控
1. Event Identification (事件識別)

• Differentiates risks and opportunities (區分風險和機會).

• Events that may have a **negative impact** (負面影響) represent risks.

• Events that may have a positive impact (好面影響) represent natural **offsets** (抵消) (opportunities), which management channels back to **strategy setting** (策略設定).

• Involves identifying those incidents, occurring internally or externally, that could affect strategy and achievement of objectives.

• Addresses how internal and external factors combine and interact to influence the risk profile.
Positive Events or News
Unforeseen Crisis or Incidents or Negative Events

Swiss NGO links Syngenta pesticide to Indian farmer deaths

The Swiss NGO Public Eye called on Tuesday for an export ban on the pesticide Polo produced by agriculture giant Syngenta, implicating it in the death of 20 Indian farmers last year.

Minister warns charities of funding cuts after Oxfam sex worker scandal

Peru's President wants the charities must show "more bedecked" amid an explosive intervention from her predecessor.
Activities 1

• Could you identify any negative news in social service organizations or other related areas?

• Spend about 5 mins to discuss with your peers

1. ______________________
2. ______________________
3. _______________________
2. Risk Assessment (風險評估)

- Allows an entity to understand the extent to which potential events (潛在事件) might impact objectives.

- Assesses risks from two perspectives:
  - Likelihood (可能)
  - Impact (影響力)

- Is used to assess risks and is normally also used to measure the related objectives.

- Employs a combination of both qualitative and quantitative risk (定性和定量風險) assessment methodologies.

- Relates time horizons to objective horizons.
2. Risk Response (風險應對)

• Identifies and evaluates possible responses to risk (識別並評估可能的風險應對措施).

• Evaluates options in relation to entity’s risk appetite (風險偏奷), cost vs. benefit (成本與收益) of potential risk responses, and degree to which a response will reduce impact and/or likelihood (減少影響和/或可能性).

• Selects and executes response based on evaluation of the portfolio of risks and responses.
Expands and elaborates on elements of internal control as set out in COSO’s “control framework.”

Includes objective setting as a separate component. Objectives are a “prerequisite” for internal control.

Expands the control framework’s “Risk Assessment”

Risk officers or Internal auditors

Monitoring (監控方式)

Recommendating improvements (改進)

Evaluating (評估)

Reporting (報告)

Examining (檢查)
Key Implementation Factors

Performing risk assessments
(進行風險評估)

Determining overall risk appetite
(確定總體風險偏好)

Identifying risk responses
(識別風險應對措施)
Identification and analysis of risks to the achievement of objectives. It forms a basis for determining how risks should be managed.

<table>
<thead>
<tr>
<th>Risk Model (Example)</th>
<th>Types of Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Environmental Risks</strong> (環境風險)</td>
<td>Capital Availability</td>
</tr>
<tr>
<td></td>
<td>Regulatory, Political, and Legal</td>
</tr>
<tr>
<td></td>
<td>Service Markets and Stakeholders Relations</td>
</tr>
<tr>
<td><strong>Process Risks</strong> (流程風險)</td>
<td>Operations Risk</td>
</tr>
<tr>
<td></td>
<td>Empowerment Risk</td>
</tr>
<tr>
<td></td>
<td><strong>Information Processing / Technology Risk</strong></td>
</tr>
<tr>
<td></td>
<td>Integrity Risk</td>
</tr>
<tr>
<td></td>
<td>Financial Risk</td>
</tr>
<tr>
<td><strong>Information for Decision Making</strong> (決策信息)</td>
<td>Operational Risk</td>
</tr>
<tr>
<td></td>
<td>Financial Risk</td>
</tr>
<tr>
<td></td>
<td>Strategic Risk</td>
</tr>
</tbody>
</table>
Risk Analysis

Source: Business Risk Assessment. 1998 - The Institute of Internal Auditors
2. Determine Risk Appetite
（確定體風險偏好）

- Risk appetite (風險偏好) is the amount of risk – on a broad level – an entity is willing to accept in pursuit of value.

- Use qualitative or quantitative (定量或定性) terms (e.g. service vs. reputation risk), and consider risk tolerance (range of acceptable variation).

Key questions:

- What risks will the organization not accept? (e.g. environmental or quality compromises)

- What risks will the social service organization take on new initiatives? (e.g. new users, new service providers, blended services)

- What risks will the social service organization accept for competing objectives? (e.g. increase service value vs. increase users’ satisfaction)
3. Identify Risk Responses (識別風險應對措施)

Quantification of risk exposure (量化風險暴露)

Options available:

- **Accept** (接受)
  - Monitor

- **Avoid** (避免)
  - eliminate *(get out of situation)*

- **Reduce** (減少)
  - institute controls

- **Share** (分享)
  - partner with someone *(e.g. insurance)*

Residual risk *(unmitigated risk 未減輕的風險 – e.g. shrinkage)*
<table>
<thead>
<tr>
<th>Impact</th>
<th>Probability</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>Medium Risk</td>
<td><em>Share</em> 分享</td>
</tr>
<tr>
<td></td>
<td>High Risk</td>
<td><em>Mitigate &amp; Control</em> 緩解與控制</td>
</tr>
<tr>
<td>Low</td>
<td>Low Risk</td>
<td><em>Accept</em> 接受</td>
</tr>
<tr>
<td></td>
<td>Medium Risk</td>
<td><em>Control</em> 控制</td>
</tr>
</tbody>
</table>

*Impact vs. Probability* (影響與概率)
# Example: Service Call Center Risk Assessment

<table>
<thead>
<tr>
<th>Impact</th>
<th>Low</th>
<th>Medium Risk</th>
<th>High Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of phones</td>
<td>Loss of computers</td>
<td>Changes in local regulations</td>
<td>Credit risk</td>
</tr>
<tr>
<td>Fraud</td>
<td>Lost transactions</td>
<td>Employee morale</td>
<td>Entry errors</td>
</tr>
</tbody>
</table>

PROBABILITY: High
Activities II - Application in social service organizations

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Risk</th>
<th>Control Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Risk</strong></td>
<td>(Low Impact, Low probability)</td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
<td>2.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
<td>3.</td>
</tr>
<tr>
<td><strong>Medium Risk I</strong></td>
<td>(Low Impact, High probability)</td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
<td>2.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
<td>3.</td>
</tr>
<tr>
<td><strong>Medium Risk II</strong></td>
<td>(High Impact, Low probability)</td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
<td>2.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
<td>3.</td>
</tr>
<tr>
<td><strong>High Risk</strong></td>
<td>(High Impact, High probability)</td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
<td>2.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
<td>3.</td>
</tr>
</tbody>
</table>
Thank You

Any Questions?
Session 3: Cybersecurity Risk Management

Cybersecurity goals
Organizational cybersecurity domains

Trainer: Mamello Thinyane
Principal Research Fellow
United Nations University

UNITED NATIONS UNIVERSITY
Institute in Macau
Cybersecurity Goals: The CIA-triad

- Confidentiality
- Integrity
- Availability
  
- Authentication
- Non-repudiation
Cybersecurity Model

Potential Attackers

- **Alice**
- **Bob**
- **Eve**
  - Passive eavesdropper
- **Heidi**
  - Mischievous designer
- **Mallory**
  - Active attacker
- **Rupert**
  - Repudiator
- **Trudy**
  - An intruder
- **Craig**
  - Password cracker
Confidentiality
Interception Attack

Examples
- Eavesdropping on communication
- Wiretapping

Mitigation
- Encryption
Integrity
Modification Attack

Examples
- Modifying, inserting, deleting information
- Website defacement

Mitigation
- Checksums
- Encryption
- Backups
Availability
Interruption Attack

Examples
• Denial of service
• Blocking access to a service
• Overloading a server
• Ransomware

Mitigation
• Replication
Authentication
Fabrication Attack

Alice

Bob

Trudy
Non-repudiation
Repudiating

I never sent the message ...

I never received the message ...

Alice

Bob
Organizational Cybersecurity Domains
Center for Internet Security Controls, 2015

Details

Recommended actions to provide specific ways to mitigate some of the most common and prevalent cyber threats facing organizations.

- 20 critical controls
- Prevent 85% of attacks by implementing just 5 controls
- 97% of attacks by implementing all 20 controls
NIST Cybersecurity Framework

Details

The framework helps businesses of all sizes better understand, manage and reduce their cybersecurity risk.

- **Framework: Identify, Protect, Detect, Respond, Recover**
- 23 categories and 108 subcategories
ISO/IEC 17799:2005

Details

Guidelines and principles for initiating, implementing, maintaining and improving information security management in organizations

- 11 domains
- Superseded by ISO/IEC27002:2013
“The organization’s mission, objectives, stakeholders, activities are understood and prioritized …

understands the cybersecurity risk to operations, functions, image, reputation, assets and individuals …
organization’s priorities, constraints and risk tolerance are established”

Key Domains: Cybersecurity Management and Policies

Clear organizational policies
Risk management
Cybersecurity roles and responsibilities are defined
Business continuity planning and management
Contacts with relevant stakeholders (e.g., CERTs) on cybersecurity matters
“The data, personnel, devices, systems and facilities that enable the organization to achieve its mission are identified and managed consistent with importance to organization objective and risk strategy”

Inventory of assets

Ownership of assets
- Including primary users

Classification of information
- Value, criticality and sensitivity

Management of removable media
- USB drives, external hard drives
“Access to assets and associated facilities is limited to authorized users, processes, or devices and to authorized activities”

- Access to network and network services
- Management of privileges access rights
- Management of passwords and credentials
  - Including password policies
- Review of user access rights
- Information access restriction
- Secure authentication
“Information and data records are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information”

- Protection from malware
- Data and system backups
  - As per backup policy
- Logging and monitoring
- Management of software acquisition, development, and maintenance
  - Software installation by users
- Audit and assessment of cybersecurity posture
- Supplier relationships and services are managed
“Personnel are aware of the relevant policies and act consistent with the cybersecurity goals of the organization”

**Prior to employment**
- Defining roles and responsibilities
- Awareness of policies

**During employment**
- Dealing with cybersecurity incidents
- Capacity-building

**Termination of employment**
- Manage the change in security requirements: access controls, devices
“The organization’s personnel and partners are provided cybersecurity awareness and training... to perform duties and responsibilities”

- General cybersecurity training
- Training on organizations policies and procedures
“Activities are undertaken to contain and limit the impact of adverse cyber incidents
organization’s response activities are improved to incorporate lessons from previous incidents
Restoration of services is coordinated with internal and external stakeholders”

- Define responsibilities and procedures
- Assessment of information security events
- Respond to incidents
- Collect relevant evidence
- Escalate and engage relevant stakeholders
The security of the physical assets to ensure use and operation that is aligned with the organizations mission and objects as well as security goals

### Defined physical perimeters and barriers
- With entry controls and procedures
- Offices, premises, rooms

### Protections against disasters
- Typhoons
- Fires
- Floods
- Earthquakes
Key Domains: Compliance

“Ensuring that the organization operates within relevant legal, regulatory and contractual requirements”

- Awareness of relevant legislation and regulations
- Understanding of the impacts and requirements on organizations operations
Thank You
Any Questions?
Session 3: Cybersecurity Risk Management

Emerging threats and effective countermeasures
Case studies

Trainer: Terry Cheung
Managing Director TopSOC Ltd
President of ISACA Macao Chapter
Our SOCaas solution won a title in Macao IT Innovation Awards organized by the Macao Computer Society and will join the APICTA (Asia Pacific ICT Awards) in Vietnam in November 2019

Many Thanks to FDCT for supporting our SOCaas project and allow us to provide One Year service to 30 SMEs
Key Success Factors

Threat Hunting

Tightly Integrated

SOAR – Demisto
- Ticketing
- Playbook
- Auto response
- CTI

Data Voyager – LogBox (SIEM)

Cyber Threat Intelligence including open source and PA
Questions to start with

What is your crown jewels?

What will be the impacts if your critical information assets are compromised?

Are you SAFE?
The Information Security Forum Protection Process

A | IDENTIFY mission-critical information assets

B | ASSESS the main adversarial threats

C | DETERMINE the required protection approaches

D | COUNTER the main adversarial threats

E | PROTECT the information life cycle
Are you at Risk?

PORTUGUESE SCHOOL IT SYSTEM HACKED FOR RANSOM

Renato Marques, MDT  Friday, August 21, 2020 - 2 Months Ago  No Comments  3.152 Views

Cathay Pacific Airlines Fined Over Data Breach

UK’s ICO Issues Largest Penalty Possible Under Country’s Older Data Privacy Laws

Aurora Yerket  VentureRx  March 5, 2020

The U.K. Information Commissioner’s Office has fined Cathay Pacific Airways £500,000 ($646,000) over a data breach that exposed the personal information of 9.4 million customers, including 111,000 British citizens, during a four-year period.

See Also: Webinar | SASE Economics: The New Frontier of Cybersecurity

The fine is the largest the U.K. privacy watchdog could impose under the country’s older data protection laws since the breach, which started in 2014 and was discovered and fixed in 2018. That happened before the EU’s General Data Protection Regulation went into effect in May 2018, according to the report.

Firewall Installed

Web Content Filtering System Installed

Intrusion Prevention System Installed

Advanced Persistence Threat or Sandbox System Installed

eMail Protection System Installed

Anti Virus or Endpoint Protection with AI Installed
Existing Cyber Security Risk

The Hacker will target any industries and any size of organizations as far as they can get money.

Whatever security protections below you have equipped, the hacker can bypass and hack your valuable assets:

- Firewall Installed
- Web Content Filtering System Installed
- Intrusion Prevention System Installed
- Advanced Persistence Threat or Sandbox System Installed
- eMail Protection System Installed
- Anti Virus or Endpoint Protection with AI Installed
Global Malware vs Malware-Free Attacks in 2019 vs 2018

Crowdstrike Global Threat Report 2020

Malware-free attacks generally require a wide range of more sophisticated detection techniques to identify and intercept reliably, including behavioral detection and human threat hunting.
Once your machine is in touch with this malware, they will call home to those C&C servers. Those servers are called Command & Control (C&C) Servers. Before the hacker attacks you, they will compromise some servers for Call Home purpose. Those servers are called Command & Control (C&C) Servers. They will code those C&C servers IPs into their newly and low profile malwares. Once the hacker is in control, they can do whatever they want.
84 anti-virus or endpoint protection vendors do not detect this malicious IP.
Hacker Kill Chain

1. Hacker hacked Command & Control Servers
2. Code the C&C IPs in their newly created low profile malware
3. Malware tries to call home (C&C) to inform hacker their success

(1) Indicates 4 files have been communicating with this IP

4 detected files communicating with this IP address

89.223.124.122 (89.223.112.0/20)
AS 31323 (United Networks Ltd.)

<table>
<thead>
<tr>
<th>Scanned</th>
<th>Detections</th>
<th>Type</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-10-22</td>
<td>27 / 71</td>
<td>Win32 EXE</td>
<td>_cache_AnubisHck1.0.exe</td>
</tr>
<tr>
<td>2020-10-22</td>
<td>53 / 71</td>
<td>Win32 EXE</td>
<td>Winos.exe</td>
</tr>
<tr>
<td>2020-10-14</td>
<td>1 / 59</td>
<td>RAR</td>
<td>Memtest86.rar</td>
</tr>
<tr>
<td>2020-10-14</td>
<td>27 / 71</td>
<td>Win32 EXE</td>
<td>AnubisCheat.exe</td>
</tr>
</tbody>
</table>

(2) 1. 4 files have been identified as malicious by different AV vendors
2. What does that mean?

(3) Hacker Kill Chain
1. Hacker hacked Command & Control Servers
2. Code the C&C IPs in their newly created low profile malware
3. Malware tries to call home (C&C) to inform hacker their success
Real Life Cases
Which one is Real?

Password Reset Request for TOPSOC.COM.MO

noreply@bluehost.com

Dear Terry,

We’ve received a request to reset the password for your hosting account at topsoc.com.mo. To reset it, simply click here or on the button below.

[Reset Password]

The link expires in 60 minutes. If you did not make this request, you may safely ignore this message. Your account remains safe and your current password will not be changed.

For tips on how to create a strong password, check out this article:
https://my.bluehost.com/hosting/help/418

Thanks,
Your Bluehost Team

Action required: Update your payment information now

Dear Customer,

Our information indicates that the payment method you used to purchase your Domain topsoc.com.mo was declined. Contact your bank for more details on the refusal of payment.

To avoid interruption of service, update your payment information now

[UPDATE YOUR PAYMENT INFORMATION]

We appreciate your prompt response to this problem and look forward to continuing to meet the needs of your business.

Connect With Us

Copyright © 2019. All rights reserved. Bluehost, 1500 North Priest Drive, 2nd Floor, Tempe, AZ 85281

We never send email unsolicited. Visit our Subscription Manager to update your preferences or unsubscribe.
Terms of Service | Privacy Notice.
Password Reset Request for TOPSOC.COM.MO

ncerplyatbluehost.com

We've received a request to reset the password for your hosting account at topsoc.com.mo. To reset it, simply click here or on the button below.

Reset Password

The link expires in 60 minutes. If you did not make this request, you may safely ignore this message. Your account remains safe and your current password will not be changed.

For tips on how to create a strong password, check out this article: https://my.bluehost.com/hosting/help/418

Thanks,
Your Bluehost Team

bluehost

Terry.

Contact: cyber-resilience@unu.edu
Analysis on the Links

URL 4:
https://u6187403.ct.sendgrid.net/ls/click?upn=YSbIkz4XBMBMyd1PzGV2kOqm5P7kpl6JOzi
mlMgLYE6XHYwRLX8xz3hgaUFeXnjPS-
2FxJZyrCRNGY7GMVkgDgDMUNdyayLlIEnYOkvxsvastESF-2BX0zJm1mDbq7WUjNTOAll5Jbt9n-
2BZzyE-2BrueBpRgYaAGPzXRxyjd4z5qYLLoqxzI-2F5oTdcu3jPHog7SKF7vyP-
2FxnNM2FknyhGBhdfLVJ-2BkAyHrT6G6tmBxHOIIhvPECOEgigrSH-
2FmYvyWFPmlKZNW311bkIGCuQse5SwSHwafeBjzijQyzaE519KSc-
3DZJW5_L6zuFFtuDGTKYGXwubUb1mAhjfHlnakWRdkTGKKejfrB1neuw13in8lb4K-
2BAg6ENFAA9b1nPqES57BdgbhsNwZGZ-2FK50tRxToUNss45tnqfAadqQ-
2B70zvMerAT8OuklYHyx2Gr8gf-2B-2F0uzow0JbgDQpwL2tWbGmnTF-
2FAENYCBYMVwttAhNIOEr6W3FgmD2Pv8V63tSgeFM8wgtbgh4ScIKejwdiH3foOmUn63foVQU-
3D

Redirected URL:
http://my.bluehost.com.web-hosting.cpllogin.ga.2.2474.deportivodelsol.com/c4ca4238a0b923820dce509a67f5849b/96
aa5d98572fdaea828b802081ff45f11/132025f557d29e851f6208f3f524999b/ffc5e01f578535f
d6f95f889cb31939d

URL 5: normal
https://u6187403.ct.sendgrid.net/ls/click?upn=LbFHhBO-2BRoFvP7gZxuPn-
2BYnFqxs3GayhbiAPTYhrU6CgCs8vuWFP-
2BxU3RyaldkFCqDheMPEi3zwCMchzkWWEBv5yz7Fpu436Q3-2BFyTOhvgB-
2BszrI1ruHI8GMBkbjO3sQLuu43RQOV9Gww-
2BpcsVK0UU9YBmz3KOWqujaMBnK54T8estH9mMhTyj3veheBc8ZuVjok4n7tcbCT2hP0ctmvbg-
3D-3D4bwv_L6zuFFtuDGTKYGXwubUb1mAhjflHlnakWRdkTGKKejfrB1neuw13in8lb4K-
2BAg6ENF75qchcebTNsIcbZH9xUuY6j7Kn4NKFo0Zk76Jx1mgjiszrq3kitoWRUEV-
2Bkb2GFxbw0Yzpldin1AWJhf2seliXv8y8fPQtCnTcrfdOd4KdTeveUDnh5RypM11OA4fu1Xbt-
7lodeD-2Foy75ktQR9epVpu06sqePw55yM8mqxltA-3D

URL 6: Facebook
https://u6187403.ct.sendgrid.net/ls/click?upn=LbFHhBO-2BRoFvP7gZxuPn-
2BYnFqxs3GayhbiAPTYhrU6CvU1r90TuawXwem7JZju-
2B70l9VkdBu4G9sSnlngTjugiGFlsweEQDmgxawBQ531ya6c9DgofYq60GHgcE8-
2FPHGUEL4jJoIq3RAHreFJmpTMS1QQM5arvOg6KO2bw5vmoX6FsDcYecY6O0b7Zwe8Kt-
Dx09ZMTjTjVCXpw0w-3D-
3DgeEc_L6zuFFtuDGTKYGXwubUb1mAhjflHlnakWRdkTGKKejfrB1neuw13in8lb4K-
2BAg6ENFhaXx-2FScYlKZmr4Vz60Ypho-
2FZ59KJn5JNexkkSuGu3HuGga1RGm15pMjzel1HLGV-
2F17dRF48ayTVil9CpTARzcraYn2jirRjeg-2Fzua8et5m6hh-2B-2Fkh76CFlVMkzRmzw-
2BPhkweF5ym1R
The Result from a Sandbox

Analysis Report http://my.bluehost.com.web-hosting.cplugin.ga.2474.de...

Overview

General Information
Sample URL: http://my.bluehost.com.web-hosting.cplugin.ga.2474.departivredesol.com/c4c4-238a-b32320.doc509146
7586b6d657269626520
19455111/1302555729a851e238
f352499b/f26a15765356/595f86b31506d

Analysis ID: 322377
Most interesting Screenshot:

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Score: 52
Range: 0 - 100
Whitelisted: false
Confidence: 100%

Signatures

Multi AV Scanner detection for submitted file
Performs DNS queries with encoded ASCII data (...
Tells to connect to HTTP servers, and all servers:
Real Life Case 2
### A Real Case from one of our customers

<table>
<thead>
<tr>
<th>Case:</th>
<th>Unknown attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP:</td>
<td>200.200.200.174</td>
</tr>
<tr>
<td>Destination IP:</td>
<td>113.108.126.3</td>
</tr>
<tr>
<td></td>
<td>113.108.127.4</td>
</tr>
<tr>
<td></td>
<td>113.108.127.16</td>
</tr>
<tr>
<td></td>
<td>124.239.128.147</td>
</tr>
<tr>
<td></td>
<td>220.189.192.2</td>
</tr>
<tr>
<td></td>
<td>61.132.87.130</td>
</tr>
<tr>
<td>Detection:</td>
<td>Command and Control (CnC) servers</td>
</tr>
<tr>
<td>Behavior:</td>
<td>Constantly connected to different CNC servers</td>
</tr>
<tr>
<td>Recommendation:</td>
<td>The source IP is 200.200.200.174, which is the most serious and was attacked several times on September 23. We recommend that the computer undergo a full virus scan and even restore the computer, and that the firewall block the following IPs from the attackers.</td>
</tr>
</tbody>
</table>

**Assessment Period:** Wed 23 Sep 2020 10:45:00 to Wed 23 Sep 2020 13:00:00 <2 hours>

**Sum:** 7 (Number of Connections)

The Hacker tried to call home but failed and tried again and again
The Solution
## Managed Security Services

<table>
<thead>
<tr>
<th></th>
<th><strong>Solution 1 (Basic) SOCaaS</strong></th>
<th><strong>Solution 2 (Advanced) Managed Security Service</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Protection</strong></td>
<td>Detection and Advisory</td>
<td>1) Detection and Advisory \ 2) Prevention, Protection and Response</td>
</tr>
<tr>
<td><strong>Pre-requisite</strong></td>
<td>Installation of our Log Collector or SIEM</td>
<td>1) Installation of SOCaaS \ 2) Equip with our supported Firewall or Endpoints (with EDR)</td>
</tr>
<tr>
<td><strong>Data to be analyzed</strong></td>
<td>Logs of firewall, AD, servers, etc.</td>
<td>1) Logs of firewall, AD, servers, etc. \ 2) Firewall and endpoint alerts</td>
</tr>
<tr>
<td><strong>What you will get</strong></td>
<td>1) Alerts and advisory \ 2) Monthly Report</td>
<td>1) Managed services for Firewall, Endpoints and SOC \ 2) Monthly Report</td>
</tr>
</tbody>
</table>

All rights reserved. These slides are prepared by Mamello Thinyane, Debora Christine, Christy Un, Farzad Sabetzadeh, Tiffany Leung, Terry Cheung, and Emil Marques as part of the Cyber Resilience Capacity Building workshop that is organized by the United Nations University institute in Macau in collaboration with City University of Macau, University of Saint Joseph, and TopSOC Ltd.

Supported by FDCT: No. 0016/2019/A

Contact: cyber-resilience@unu.edu
**Benefits of SOCaaS & Managed Services**

**SOCaaS**
- Visibility of your environment
- 24*7 detection and alerts
- Professional advisory with recommendations
- Monthly security report to show your healthiness status

**Managed Firewall & Endpoint Services**
- Enable Prevention and Protection (Full protection)
- Highly integrated to facilitate better detection and response
- Managed by skillful security professional and processes to minimize lack of resource issue
- Monthly security report to show your healthiness status including firewall and endpoint
1) Capture Logs from firewall or Wifi Router
2) Enable Bro to sniff traffic
Thank You

Any Questions?
Session 3: Cybersecurity Risk Management

Socio-technical cyber threats and countermeasures
Organizational impacts

Trainer: Debora Christine

Research Assistant
United Nations University
Social
Technical
Environmental
Personal
Organizations are **complex socio-technical systems**: comprising social, technical, and environmental practices.

Socio-technical cyber threats exploit the **vulnerabilities** at the intersection of organization’s social, technical, and environmental practices.

Need to address **socio-technical gaps** within organizational cybersecurity practices.
Socio-technical cyber threats

- Influence threat
- Availability threat
- Interception
- Confidentiality threat
- Abuse
- Authentication threat
- Institutional threat
The use of psychological manipulation to trap users making security mistakes or overlook associated risks to either inject a malware or retrieve sensitive information that may be used for fraudulent purposes.

Social engineering

- **Baiting**: offer of free items
- **Phishing**
- **Pretexting**: using pretext to build a sense of trust
- **Quid pro quo**: offer of free services
- **Tailgating**: asking for access to a restricted area of an organization's physical or digital space
Social engineering - Phishing

Any attempt to trick individuals to share sensitive information, such as passwords, usernames, and credit card details for malicious reasons using a message sent via email, text, phone call, or direct-chat message that appears to be from a trusted source.”
Social engineering - Countermeasures

Never respond to any spam

Anti-spam filters

Don't press buttons or respond to prompts. If you get an automated message that asks you to press buttons or respond to questions, don't do it.

Ask questions.

Don’t give out any personal information until you have verified whether the person sending the message/calling is legitimate.

Report incidents
Online scams and frauds

“The use of ICTs to defraud or take advantage of targets, typically financial gain.”

e.g. identity theft, non-delivery payment, quick-money promise, and online advertising fraud.
Online scams and frauds - Countermeasures

Don’t open suspicious texts, pop-up windows or click on links or attachments in emails – delete them.

Don't respond to requests asking for remote access – hang up.

Multilayered security features
- (e.g. password protection, multi-factor authentication, update security software, back up data)

Research the organization.

Perform online payments only on secure websites.

Contact the bank immediately if fallen for a scam and report it.
Insider threats

Malicious insider: An insider who intentionally abuses legitimate credentials maliciously to steal information for financial or personal gains.

Compromised insider: An insider whose account credential has been harvested and unintentionally enables an attacker to access sensitive information or resources.

Careless insider: people who make the most common mistakes and generally do not pay significant attention to the security practices of the organization.

“Security risks that originate within the targeted organization. The actor could be current staff, former staff, consultant, or board member.”
Insider threats - Countermeasures

- Privileged access management (e.g. password)
- Access, authentication, and account change logs
- Secure backup and recovery processes
- Anonymous, confidential mechanism for reporting security incidents
- Post-employment process (e.g. NDA)
- Insider threat awareness training
# Impacts on organizations

<table>
<thead>
<tr>
<th>Category</th>
<th>Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical/digital assets</td>
<td>Damaged/unavailable, destroyed, corrupted, reduced performance</td>
</tr>
<tr>
<td>Economic</td>
<td>Financial loss, fines, compensation payment, disrupted operations</td>
</tr>
<tr>
<td>Reputational</td>
<td>Damaged public perception, under scrutiny</td>
</tr>
<tr>
<td>Psychologica  l</td>
<td>Embarrassed, loss of confidence, guilty</td>
</tr>
<tr>
<td>Social/societal</td>
<td>Drop in organization’s morale</td>
</tr>
</tbody>
</table>

---

**Caritas Hong Kong support centre apologises after losing data on over 100 PolyU students**

**UNICEF data leak reveals personal info of 8,000 online learners**

*By Vince Chadwick // 09 September 2019*

---

**Attackers targeting non-governmental organizations in Myanmar with new ‘KillISomeOne’ backdoor**

Operators used four different DLL side-loading scenarios to install and execute new malware after removing a resident PlugX Backdoor.

---

*WARNING!*  

*ALERT!*
Socio-technical cyber threats - Countermeasures

- Awareness about organization’s cybersecurity risks and compliance requirements.
- Capacity-building to recognize and report suspicious activities.
- Training in cybersecurity risk prevention.
- Restrict the use of personal computers, mobile devices, and email accounts to access organization information.
- Password management policy/training.
- Multifactor authentication.
Thank You

Any Questions?
Session 4: Local Cybersecurity Landscape

Trainer: Emil Marques
Senior Lecturer
Faculty of Business and Law
E-government Workgroup in 2005

- SAFP
  - Deputy Director
- Management Team
- Technical Team
- Portal Team
Public Administration and Civil Service Bureau reorganization

Before 2011/08/08 – Decreto-Lei n.º 23/94/M de 9 de Maio

- **eGov WG**
  - Grupo de Trabalho do Governo Electrónico
    - (Electronic Government Working Group)

- **DMA**
  - Departamento de Modernização Administrativa
    - (Department of Administrative Modernization)

- **DI**
  - Departamento de Informática
    - (Information Technology Department)

From 2011/08/08 – Regulamento Administrativo n.º 24/2011

- **DAGE**
  - Departamento dos Assuntos do Governo Electrónico
    - (Electronic Government Affairs Department)

- **DDFO**
  - Departamento do Desempenho e Funcionamento Organizacional
    - (Dep. of Performance and Organizational Functioning)
Portal for Civil Servants

Macau vs. HK

**Macau**

- SAFP
- DAGE
- DDFO

**Hong-Kong**

- OGCIO: Office of the Government Chief Information Officer
- EU: Efficiency Unit
- STC: Standards and Testing Center Ltd.
Endereço: Rua do Campo, n.º 162, Edifício Administração Pública, n/c, 11.º - 12.º andares e 21.º - 29.º andares, Macau
Telefone: (853)2832 3623 Fax: (853)8987 1722
E-mail: info@safp.gov.mo

| Departamento do Assuntos do Governo Electrónico (DAGE) |
| Telefone: 8987 1095 / 2833 9959 |
| Fax: 2835 5402 |
| Email: dage@safp.gov.mo |
| Endereço: Rua do Campo, n.º 162, Edifício "Administração Pública", 25.º andar, Macau |

| Divisão do Planeamento e Infra-estruturas do Governo Electrónico (DPIGE) |
| Telefone: 8987 1095 / 8987 1514 |
| Email: dpige@safp.gov.mo |

| Divisão da Aplicação de Informação e Desenvolvimento do Governo Electrónico (DAIDGE) |
| Telefone: 8987 1095 / 8987 1077 |
| Email: daidge@safp.gov.mo |
In order to align with the Macao Sp its development, CTT has been p scheme (abbreviated as Common registration procedure for the “Common Civil Service Bureau (SAFP) or the SEPBox services, and receive a eSignCloud account via the corre electronic signatures with legal effe services in the website or mobile a conjunction with eSignTrust’s on authentication. Citizens can also b account of common access through

Starting from 2019, CTT provides domestic workers from the Labour service for food and beverage est
### Legislation in relation to Cyber Security

<table>
<thead>
<tr>
<th>有關法律／批示</th>
<th>名稱</th>
</tr>
</thead>
<tbody>
<tr>
<td>第2/2020號法律</td>
<td>《電子政務》 Electronic Governance</td>
</tr>
<tr>
<td>第13/2019號法律</td>
<td>《網絡安全法》 Cybersecurity</td>
</tr>
<tr>
<td>第4/2020號法律 修改第11/2009號法律</td>
<td>《打擊電腦犯罪法》 Law against Cyber Crimes</td>
</tr>
<tr>
<td>第301/2007 號行政長官批示</td>
<td>《公共行政改革路線圖》 Public Administrative Reform Road Map</td>
</tr>
<tr>
<td>第7/2007 號行政法務司司長批示</td>
<td>開設電子郵箱收發電子公函批示 Official Electronic Correspondence and Email</td>
</tr>
<tr>
<td>第8/2005 號法律</td>
<td>《個人資料保護法》 Personal data protection Law</td>
</tr>
<tr>
<td>第5/2005號法律</td>
<td>《電子文件及電子簽名》 E signature Law</td>
</tr>
</tbody>
</table>
PDPA - Personal Data Protection Act (2005)

Personal data processed lawfully and respect principal of good faith

Purpose – limitation Principle

Principle of proportionality

Accuracy Principle

Data Retention Period

Adopted on August 4th 2005

Came into effect on February 19th 2006
Article 3: section 1 – manual filing of personal information

Article 3: section 3 – applies to video surveillance and other forms of capture, processing and dissemination of sound and images allowing persons to be identified.

Article 5: Section 1 – Subsection 5 – kept for no longer than is necessary and for the purpose of which they were collected.

Article 6: Criteria for making data processing legitimate

Article 15 – Security of processing
Article 15 - Security of processing

Section 1: Controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access in particular where processing involves the transmission of data over networks,....
PDPA - Legal Framework

Government

Firms

NGOs
• Defined **critical infrastructure** as information networks and computer systems as important to the functioning of society in Macau.

• Defined explicitly operators and **Providers of critical infrastructure**: Private and Public

• Defined a special class called the **Internet Service Providers**
Regulamento Administrativo n.º 35/2019

委員會 (CPC)

网络安全事故预警及应急中心 (CARIC)

Public Administration and Civil Services Bureau
Judicial Police
Macao Post and Telecommunications Bureau
Private critical infrastructure operators:

- Private entities that are qualified to operate and provide services to the administration and operate in the following areas:
  - Banks, Financial Entities and Insurance Institutions, Games of Fortune operators, Sea / Land / Air Transportation Operators, some Utilities Operators, Healthcare Operators, Public Capital Companies, etc.
Lei No. 13/2019
Cybersecurity Law

Series of laws, regulations and guidelines implemented over time

Different guidelines for different industries defined in the law

Additional updates will be implemented
What we know so far Art. 4

- Water Supply
- Banks, Financial and insurance institutions
- Health care provisions in hospitals
- Sewage and garbage collection and treatment
- Wholesale supply of fuel and food for sanitary and phytosanitary
- Statutory slaughter houses
What we know so far Art. 4

Supply and distribution of electricity and natural gas

Sea, land and air transport operators

Television and sound broadcasting

Gaming operators

Fixed and mobile public telecommunications network operators

Companies owned by the government

Public administrative corporations activities limited to science and technology
Cyber Security - Legal Framework

Government
Office of CE
Principal Officials
Public Sector
Public legal persons

Firms
Banks
Insurance Co.
Land, Air and Sea
CEM
ISP eg. CTM

NGOs

Cyber Resilience Challenges
What we know so far Art. 4

Macau Community Centers

- Tutoring Centers
- Medical Clinics
- Community assistance (subsidy/government application)
- Macau Health Services Subsidy
- Continuing Education Subsidy Application
- Any other services?
Information needed for processing procedure

- Macau ID (Original / ID Copy)
- Files containing personal info (access / security)
- Employee Access rights (Who can see the data)
- Trust in the system
**Possible Compliance requirements in the future**

<table>
<thead>
<tr>
<th>Organization (art. 10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedures (art.11)</td>
</tr>
<tr>
<td>Assessment and Report (art.12)</td>
</tr>
<tr>
<td>Cooperation (art.13)</td>
</tr>
</tbody>
</table>
**Organization obligations**

1. Setup cybersecurity unit with organization
2. Provide human and financial resources
3. Appoint personnel with necessary skills in charge of this function
4. Recovery and response contact point for CARIC
5. Procedures for complaint and follow up
6. Annual report
Thank You

Any Questions?
In Conclusion

Mamello Thinyane
Cyber Resilience phases

1. PREPARE
   Awareness-raising
   Capacity-building
   Redundancy measures
   Recovery plan
   Logging and monitoring
   Prevention measures
   Active mediation
   Web hygiene
   Attitudinal measures...

2. ABSORB
   Alternative resources
   Withstand measures
   Incident reporting
   Threat removal measures
   Sandboxing and isolation
   Engage measures

3. RECOVER
   System recovery
   Account recover
   Data recovery
   Professional support
   Social support

4. ADAPT
   Evolve measures
   System upgrades
   Resource swapout
   Bounce forward
   Enhanced capacity
Going Forward

Cyber Resilience Capacity Building

- Introduction to Organizational Cyber Resilience Management
- Everyday Cybersecurity in Organizations
- Introduction to Cybersecurity Support in Organizations

More workshops planned for 2021

Target to provide training for directors / managers of other third-sector organizations in Macau

Training for “IT-related” personnel in organizations

Training for general staff in organizations
“Enhancing the resilience of civil society in smart digital futures”

cyber-resilience@unu.edu
The Team

Mamello Thinyane
Principal Research Fellow
United Nations University

Debora Christine
Research Assistant
United Nations University

Christy Un
Visiting Research Assistant
United Nations University
THANK YOU

UNITED NATIONS UNIVERSITY
INSTITUTE IN MACAU
Estrada do Engenheiro Trigo No 4, Macau SAR

Contact:
cyber-resilience@unu.edu

Acknowledgement:
This work is supported by the Science and Technology Development Fund of Macau (FDCT) under Grant No. 0016/2019/A