# MANAGING SECURITY INCIDENT RESPONSE DURING COVID OUTBREAK

## *A LESSON LEARNED*

OIC-CERT ONLINE TRAINING 2020 – SEPTEMBER 2020

**Fetri Miftach,** PhD CEng MBCS CITP

World Health Organization

Health Topics | Countries | Newsroom | Emergencies

Home / Newsroom / Detail / WHO reports fivefold increase in cyber attacks, urges vigilance

# WHO reports fivefold increase in cyber attacks, urges vigilance

23 April 2020 | News release | Geneva

Since the start of the COVID-19 pandemic, WHO has seen a dramatic increase in the number of cyber attacks directed at its staff, and email scams targeting the public at large.

This week, some 450 active WHO email addresses and passwords were leaked online along with thousands belonging to others working on the novel coronavirus response.

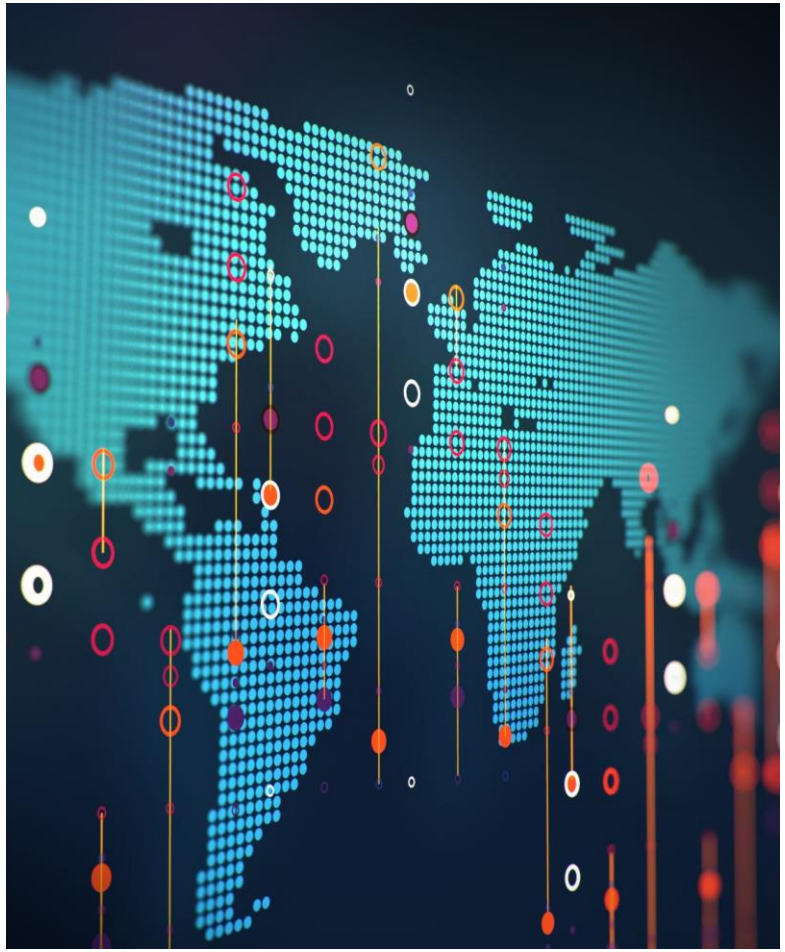
The leaked credentials did not put WHO systems at risk because the data was not recent. However, the attack did impact an older extranet system, used by current and retired staff as well as partners.

# CHALLENGES THAT BUSINESSES HAVE TO DEAL WITH …1

- Businesses are forced to change how they operate and these would typically affect underlying ICT infrastructure. Under normal circumstances the modifications would go through structured processes, including **risk analysis**, **security testing** and **configuration management**, however, due to time constraints, these were either sidestepped or fasttracked for the sake of formality.
  - Without proper architecting process, these changes degraded the overall security profile and system administrators quickly found it difficult to identify where the problems occurred – also note that resource constraints also means required corrections may be delayed.
  - Over time, the gaps between previously validated baseline security configuration and current as-implemented configuration could give rise to critical vulnerabilities.

# CHALLENGES THAT BUSINESSES HAVE TO DEAL WITH …2

- Infrastructure boundaries were often **redrawn and extended** to cater for alternative work locations, new access profiles, third party services requiring additional access channels, and the use of cloud services.
  - Difficulties in ensuring effectiveness and consistency of security control implementation across these services.
  - Visibility of new boundaries may be limited – difficulties in prioritizing the already stretched security administration resources.



# CHALLENGES THAT BUSINESSES HAVE TO DEAL WITH …3

- With the majority of personnel working remotely (quite often including some security operations staff), the new immediate focus is to **secure** and **monitor endpoints** in diverse end-user environments.
  - Lack of technical supports to solve problems with company-supplied laptops lead to the use of personal devices with less-than adequate security configuration.
  - With home networks usually shared with other members of the family, security operations are hard pressed to prevent direct attacks to endpoints that are outside of their monitoring scope.
  - At the same time, attack patterns shifted from trying to find and exploit obscure vulnerabilities in a well-defended corporate infrastructure, to reusing proven TTPs against typical home networks.

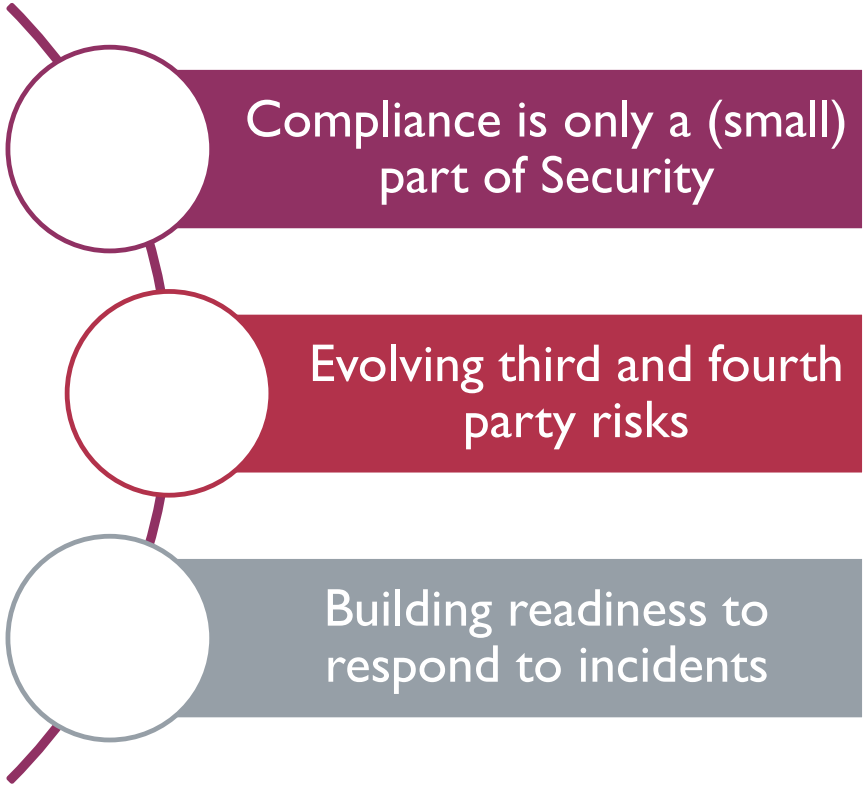
# CHALLENGES THAT BUSINESSES HAVE TO DEAL WITH …4

- Supply Chain partners are also bearing the brunt of economic downturn – if a typical business has to **reallocate priorities**, including budgets previously set aside for **cyber security improvements**, supply chain partners may be experiencing the same, if not worse, constraints.
  - The vulnerabilities in their system provide a more attractive (and easier to exploit) target – many businesses do not tightly control and monitor authorized/trusted third party access,
  - Contractual SLA and security-related clauses are not effective preventive controls in this situation.

# INDUSTRIES AT RISK

- Food supply chains
  - retailers
- Hospitals
  - medical research laboratories,
  - vaccine research labs,
  - clinical trial administrators
- Pharmaceuticals

- Companies who are lagging behind in coping with WFH-era



# CASE: FINANCIAL SECTOR (INSURANCE)

- Incident:
  - Spear Phising attack targeting internal staff (finance department)
  - Attacker spent some time learning how the company's finance department operated, observed its business partners and procurement patterns
  - Attacker then sent a well-crafted invoice for delivery of certain products and services through a series of emails, spoofing the sender's addresses and satisfied subsequent queries to verify the payment request
  - Losses: Over USD$150.000

# CASE: FINANCIAL SECTOR (INSURANCE)

- Conditions prior to incident
  - A high number of spear fishing emails sent to company staff were later discovered from incident analysis and forensics
  - Some of the staff who received the spear fishing emails confessed that they "felt" something was not quite right, but decided to ignore it due to various reasons (workload, difficult to access IT staff, ...)
- The business partner whose identity was used during the attack, was also a victim
- Corrections/Improvement:
  - Company have since implemented Mail filtering mechanisms as well as regular security awareness

# CASE: FINANCIAL SECTOR (BANK) & FMCG

- Incident:
  - Ransomware infection (Ryuk and BeijingCrypt)
  - Initial attacks through brute force RDP and spear phishing emails
  - Impact: data in dozens of criticsl servers were encrypted and business operations crippled for several days.
- Conditions prior to incident
  - Even though existing BCPs include scenarios related to malware attacks, they have not been updated to reflect WFH conditions

LESSONS LEARNED

# USER BEHAVIOUR

- Increased use of social media sites and a proportionally increased number of social media-related security events from exposure to phishing and social engineering attacks.
- Significant increase in the use of video teleconferencing services with associated vulnerabilities and unintentional information leaks from accessing these services.
- Increased browsing of COVID-19 news articles and related developments such as countless topics related to "new normal," leading to browser-based attacks from malicious websites hosting fake news and graphical dashboards of global pandemic status.
- WFH environments and less restrictive (poorly defended) home networks induce a false sense of security and reduced vigilance about online hygiene while working remotely – in contrast, being physically in an office may provide a different "secure" mindset.

LESSONS LEARNED

# NEW OPPORTUNITIES FOR CRIMES

- Criminal actors understand the *opportunities* presented to them:
  - User behavior during the pandemic and working from home period manipulated to custom phising attacks.
  - Attack or exploit techniques that were no longer effective to use against fortified corporate networks may be successfully used to gain access to home networks and computers, leading to theft of data or pivot into internal segments.
  - *Intelligence* capabilities are present in criminal groups, often offered for purchase in a CaaS scheme. The capabilities allow them to detect changes to configurations and platforms as well as overall degradation in security profile, especially during pandemic period.

LESSONS LEARNED

# HUMAN FACTOR OF SECURITY OPERATIONS & CSIRT STAFF

- Considered "essential" and required to continue working full time, in contrast to colleagues who are given the choice to telework or work under reduced hours during stay-at-home orders
- Additional workloads during pandemic (analysing data, reviewing alerts, and addressing security incidents) may tax already-stretched security personnel
- Some incident response activities necessitate onsite presence, thus requiring CSIRT personnel to continue working at customer sites – in these circumstances, personal safety and higher risk of exposure must be given serious considerations
- Internal company network activities may be significantly reduced due to reduced staff presence or active hours, as well as lower than normal-level access to some enterprise resourcesm – this provides some respite to security staff, however the usual mistakes and poor security practices by end users are now taking place at their homes, well away from monitoring and detection mechanisms

LESSONS LEARNED

# UNDERSTANDING OWN CONSTRAINTS

- It is important for businesses to understand the extent of vulnerabilities visible to external parties.
  - Internal resources may be limited and focused on protecting known systems and mitigating identified vulnerabilities – but would-be **attackers can see much more from the outside**.
  - Any vulnerability information may be traded, sold, passed around and used as part of a long-term attack campaign - they maybe used to test the readiness of security operations to detect and respond to attack patterns – failure of which provide additional latitude for the attacking party.

LESSONS LEARNED

# ESTABLISHING NEW BASELINES

- Since users are now working remotely, using different services, doing more personal browsing on their work computers, and generating a different volume of network traffic and events, the baseline for normal network activity has completely changed.
- The new baseline will have to be analysed to update or create new monitoring rules, set up detection alerts, formulate specific dashboards, and the need to look and understand new anomalies that fall outside the baseline.
- If a company decides to implement a long-term strategy on migration to remote activity, new policies will have to be drawn up to regulate self-defined protection regimes that may be implemented by employees at their home. For example, a security-conscious staff may employ personal VPN services for secure browsing, and these VPN services have diverse geographic exit points. If this user connect to the company's network from a foreign location not commonly seen, this could raise an alert that needs to be investigated.

IMPROVING READINESS OF CSIRT

# INCIDENT PREVENTION – RAISING AWARENESS

- A senior member of the security team should be part of the company's pandemic crisis management working group to provide guidance on security concerns and business-risk-appropriate advice.
- Reinforce the need for remote workers to remain vigilant to socially engineered attacks.
- Employees will have more distractions than usual when working away from the office, whether it's dealing with family members at home or concerns about their own health. They're also operating in a different environment, and might not be as vigilant about security during a time where cybercriminals will exploit the chaos.
- Ensure you that senior leaders are well informed with the risks of targeted phishing attacks, and alert all employees to the escalating cyberthreat environment. Remind everyone that they must be hypervigilant to suspicious activities.
- Where possible, issue reminders regularly on location of pertinent documents such as remote and mobile working policies, as well as where they can access security awareness training material if they want a refresher.

IMPROVING READINESS OF CSIRT

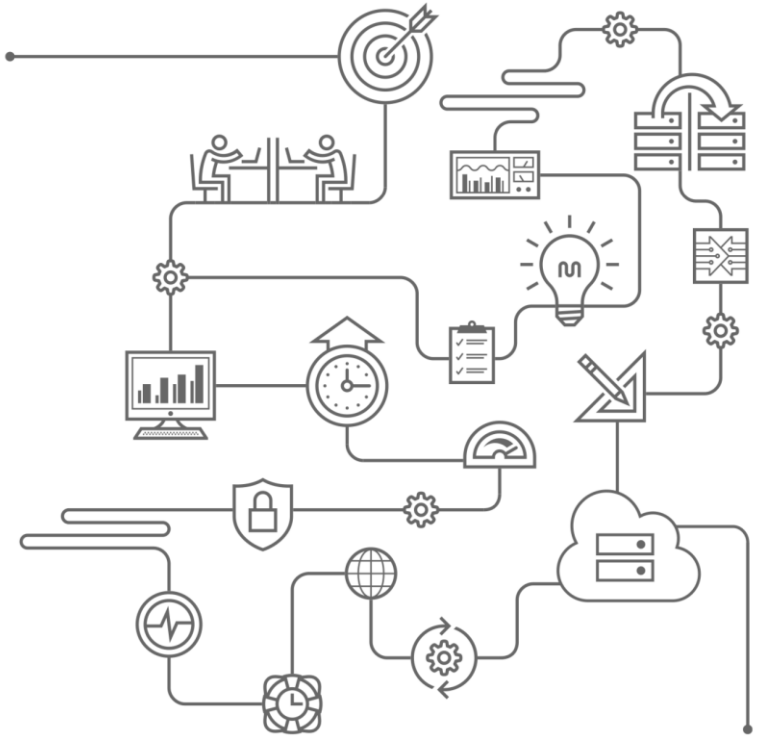
# INCIDENT PREVENTION – USER ACTIVITIES

- Identify and monitor high-risk user groups within the company. High-risk users should be identified and monitored for anomalous such as unusual bandwidth patterns or bulk downloads of enterprise data to identify possible security breaches.
- Ensure that users can easily interact with internal security teams, such that they can quickly ask questions, when unsure about security-related issues, report incidents in real time, and at the same time, be informed of good security practices practices.
- Remind users of using approved messaging, file-transfer, and document-management tools. Company-supplied or approved devices should.be used at all times when conducting company business.

IMPROVING READINESS OF CSIRT

# SUPPORTING USER ACTIVITIES

- Look into capability to allow secure remote-working.
- IT help desks should add capacity or complemented (integrated) with security-team members temporarily at call centers to provide added frontline support.
- Ensure effectiveness of incident-response protocols and fraud-prevention capabilities for any new business processes that might have been implemented in haste during pandemic period.
- When responding to cybersecurity incidents, normal escalation pathways must not interrupted because people are working from home.



IMPROVING READINESS OF CSIRT

# CONTROLLING EXTENDED ACCESS

- Ensure that all remote access capabilities are tested for security and continuously monitored.
- Allocate additional resources to ensure that endpoints used by workers are patched, remind users to always practice endpoint hygiene and for those who could not avoid using personal devices, extra attention and support should be provided.
- Extra monitoring should be implemented on access to corporate applications that store mission-critical or personal information, especially from personally owned devices.
- Where possible, personal devices should be checked and confirmed to have adequate anti-malware capabilities installed and enabled.
- Other mechanisms such as software-token based multifactor authentication will also be useful to ensure only authorized personnel have access to corporate applications and information remotely.

IMPROVING READINESS OF CSIRT

# MONITORING

- Ensure security monitoring capabilities are reconfigured to have visibility of the expanded operating environment
- Be aware that the potential for cybersecurity teams to miss events is far higher from sudden relocation of much of the workforce (including security and risk management teams) to remote locations.
- Ensure that any existing monitoring tools and capabilities are providing maximum visibility. Check that internal security monitoring capabilities and log management rule-sets enable full visibility.
- If the company is relying on managed security services providers, discuss and confirm that their monitoring and logs have been adapted to take into account the new operating landscape.

IMPROVING READINESS OF CSIRT

# INCIDENT RESPONSE PROCESSES

- Ensure that the organization's incident response protocols reflect the altered operating conditions and are tested at the earliest instance.
- Assuming that most of the security operations team and CSIRT are now working in completely different environments and mindsets, incident response plans and protocols might no longer be effective, or they may even be obsolete, needing immediate adjustment. Even incidents that would normally be understood and well-managed may become complex if the team cannot respond effectively.
- Ensure that all CSIRT roles are assigned with alternatives, and that everyone has access to resources they need to be able to respond to incoming incident information effectively.
- Review all documentation and conduct a walk-through with a specific focus on finding any problem areas due to changing operating environment.

IMPROVING READINESS OF CSIRT

# RESOURCES REQUIRED FOR INCIDENT RESPONSE

- Check that CSIRT framework can be used to co-ordinate incidents remotely and that necessary conferencing/coordination facilities as well as access to incident management sites/processes are adequate.
- A pre-prepared/pre-defined virtual war room should be setup in case physical access is limited or restricted.
- If the are key individuals involved in the incident response, try to reassign roles or source additional talents internally to reduce that dependency.
- Decision makers may not be reachable during an incident response or recovery process, discuss with appropriate parties (legal, risk) to agree on alternative authorities.
- Discuss and formulate response plan for a widespread ransomware incident when large parts of the company's workforce are working from home. Ensure that reponse plans are still effective for all other incident scenarios that have been analysed.

# THANK YOU