IGF 2023
Best Practice Forum on Cybersecurity

Lessons from cybersecurity events to inform cybersecurity policy and norms deliberations

Output document

November 2023

Acknowledgements

The *Best Practice Forum Cybersecurity (BPF)* is an open multistakeholder effort conducted as an intersessional activity of the *Internet Governance Forum (IGF)*. This report is the draft output of the IGF 2023 BPF on Cybersecurity.

The BPF output is the product of the collaborative work of many, who participated in BPF virtual meetings and online discussions, or provided input on the mailing list or requests for feedback. The BPF presented a draft of this output document at the IGF 2023 in Kyoto, Japan. This final version takes into account feedback on the draft.

BPF Cybersecurity coordinating team

Mr Bart Hogeveen, *BPF Co-facilitator*
Mr Klée Aiken, *BPF Co-facilitator*
Ms Ellie McDonald, *BPF Co-facilitator outreach*

Ms Hariniombonana Andriamampionona, *BPF MAG Co-facilitator*
Ms Carina Birarda, *BPF MAG Co-facilitator*
Ms Josephine Miliza, *BPF MAG Co-facilitator*

Mr Wim Degezelle, *BPF Consultant, IGF Secretariat*

Key contributors to the report and, or the BPF session at IGF2023 Dr Allison Wylde, Mr Dino Cataldo Dell’Accio, Ms Eleanor Sarpong, Ms Ellie McDonald, Mr Eugene Tan, Ms Helena Huang Yixin, Mr Kivuva Mwendwa, Ms Louise Marie Hurel, Ms Susan Garae, Ms Ying Chu Chen, Ms Cherie Lagakali, Ms Jessica Woodall.

www.intgovforum.org/en/content/bpf-cybersecurity

Disclaimer:

The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.

Table of Contents

Executive Summary

Lessons from cybersecurity events to inform cybersecurity policy and norms deliberations

Cybersecurity events and the experiences of first responders and those most affected provide valuable input for those involved in high-level cyber policy discussions and the development of cyber norms. At the end of the day, these policies and norms must make a difference in the lived experience of the people directly affected by or responding to incidents.

The IGF Best Practice Forum on Cybersecurity (BPF Cybersecurity) in 2021 found that the cyber norms we have today would have helped mitigate many of the notorious cyber events of the past (IGF 2021 BPF Cybersecurity, *The use of norms to foster trust and security.*). This analysis also uncovered a missing nuance in norms and policy that could be obtained from deeper stakeholder involvement and the experiences of those most affected. As part of its activities in 2022, the BPF explored how storybanking can help to better understand events and lifting voices of those directly involved.

This year, the BPF Cybersecurty 2023, based on the previous work, evaluated cybersecurity events with the objective to present first-person experiences and narratives from those affected as victims or first responders to policy and norms developing deliberations, so that high-level policy decisions are grounded in reality. The BPF asked the community, via an open survey, what cyber incidents it is most concerned about and then selected a shortlist of events for a deeper analysis by volunteer groups. The BPF draft findings (Oct 2023) were discussed at the BPF session at the IGF 2023 annual meeting in Kyoto (12 October).

The following cases have been explored: *2022-2023 Black Axe cyber criminal activities*, *2022 ransomware incidents in Costa Rica*, *2021 Medibank incident*, *ransomware incidents in the Pacific in 2021-2023*, and the *2020 Solarwinds breach.*

Observations and trends that emerged from the analysis.

- Discussions around major cyber incidents often revolve around the technical, financial, legal, and intergovernmental consequences. However, the opportunities and challenges presented across the cyber ecosystem ultimately lie with the public, whether individuals or societies affected directly by a cyber incident or through the resonating impacts of an incident. (e.g. impact on human services, privacy and data concerns, flow-on effects and impact of cyber incidents beyond the technical or service delivery space).

- Regardless of any attributions in the cases examined, there are clear norms that could be directly applied to prevent, respond, or mitigate the impacts of the incidents explored. (e.g. interstate cooperation on security, respect for human rights, cooperation to stop crime and terrorism, respond to requests for assistance, report ICT vulnerabilities, cyber capacity building).

- Cyber capacity building is the most prominent theme across the incidents explored, with the need for further cyber capacity building activities made clear and in many cases acted upon.
  More significantly however, many of the incidents explored showcased the positive impact of previous cyber capacity building activities on economies' and organisations' ability to respond to the incidents themselves. (e.g. established networks of trust and information sharing, or trainings that allowed and facilitated local teams to be able to respond).

Concluding remark.
The BPF work saw early themes developing across the cases examined. It is, however, still very much a starting point for wider investigation seeking to ground discussions of international norms in real incidents and inform them on the wider impacts cyber incidents can have on the everyday lives of citizens, regardless of State or non-state involvement.

The Report of the IGF 2023 Best Practice Forum Cybersecurity is available at
https://www.intgovforum.org/en/filedepot_download/56/26668

Introduction

The IGF Best Practice Forum on Cybersecurity

The Internet Governance Forum (IGF), convened by the United Nations Secretary General[1], brings stakeholder groups together as equals in discussions on public policy issues relating to the Internet.

To enrich the potential for IGF outputs, the IGF has developed an intersessional programme of Best Practice Forums (BPFs) intended to complement other IGF community activities.

Since 2014, IGF Best Practice Forums have focused on cybersecurity related topics. In the last five years, the BPF on Cybersecurity started investigating the concept of *culture, norms and values in cybersecurity*.

In 2018 the BPF took a closer look at norms development mechanisms. In 2019, when the BPF ran in conjunction with the initiation of UN GGE and OEWG, the BPF looked at best practices related to the operationalization of cyber norms and started analysing international and cross-stakeholder cybersecurity initiatives for commonalities. In 2020, the BPF took a wider approach and explored what can be learned from norms processes in global governance in areas completely different than cybersecurity, and continued and further advanced the analysis of cyber norms agreements. In 2021 and 2022 the BPF Cybersecurity investigated more deeply the drivers behind, and disablers of, cyber norms, while a second work stream tested norms concepts against historical Internet events to understand how specific norms have or would have been effective at mitigating adverse cybersecurity events. Last year's BPF also explored the value of storybanking cybersecurity incidents, and produced an ad hoc mythbusting paper on the difference between cybercrime and cybersecurity from a policy perspective.

[1] Resolution adopted by the UN General Assembly on 16 December 2015, (70/125), extending the IGF's mandate set out in par. 72 to 78 of the Tunis Agenda. https://unctad.org/system/files/official-document/ares70d125_en.pdf

IGF Best Practice Forum on Cybersecurity - past work and outputs

- Ad hoc paper *'Mythbusting: cybercrime versus cybersecurity'*[2] and Consolidated output 2022 BPF Cybersecurity (IGF 2022)[3]
- The Use of Norms to foster Trust and Security (IGF 2021)[4]
- Exploring Best Practices in Relation to International Cybersecurity Initiatives (IGF 2020)[5]
- International Cybersecurity Agreements (IGF 2019)[6]
- Cybersecurity Culture, Norms and Values (IGF 2028)[7]

[2] https://www.intgovforum.org/en/filedepot_download/56/24126

[3] https://www.intgovforum.org/en/filedepot_download/56/24125

[4] https://www.intgovforum.org/en/filedepot_download/235/20623

[5] https://www.intgovforum.org/en/filedepot_download/10387/2397

[6] https://www.intgovforum.org/en/filedepot_download/8395/1896

[7] https://www.intgovforum.org/en/filedepot_download/6764/1437

IGF BPF 2023 - Inform cybersecurity policy and norms deliberations through lessons learned from cybersecurity events

Objective

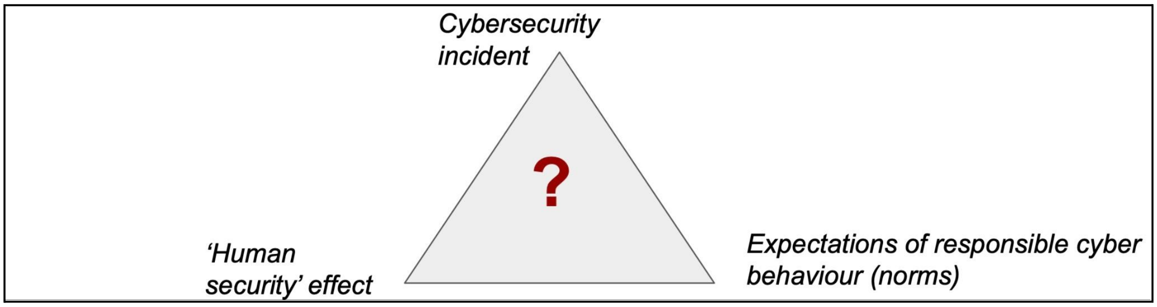
Cybersecurity events and the experiences of first responders and those most affected provide valuable input for those involved in high-level cyber policy discussions and the development of cyber norms. At the end of the day, these policies and norms must make a difference in the lived experience of the people directly affected by or responding to incidents.

The BPF Cybersecurity in 2021[8] took a closer look at notable cybersecurity events of the past to assess if norms would have made a difference, and found that the cyber norms we have today would have helped mitigate many of the notorious cyber events of the past. This analysis also uncovered a missing nuance in norms and policy that could be obtained from deeper stakeholder involvement and the experiences of those most affected. As part of its activities in 2022, the BPF explored how storybanking can help to better understand events and lifting voices of those directly involved.

This BPF 2023, based on the work in previous years, is collecting and evaluating cybersecurity events with the objective to present first-person experiences and narratives from those affected as victims or first responders to policy and norms developing deliberations, so that high-level policy decisions are grounded in reality.

[8] IGF 2021 BPF Cybersecurity, *The use of norms to foster trust and security.* https://www.intgovforum.org/en/filedepot_download/235/20623

Figure 1: Objective of the BPF, connect reality of 'human effects' with the development 'normative expectations'



Work plan & methodology

The BPF discussed[9] two possible approaches to collect and unpack incidents, both driven by crowdsourced analysis from the BPF community:

- Option 1**:** collect high-profile cases and select one incident per region for analysis of its impact and assess the effect of the observation of norms and their implementation.
- Option 2**:** unpack 2 or 3 high-profile international incidents that are well documented, produce an incident and response timeline, and determine the impact of cyber norms and policies.

The first option was retained as methodology and the BPF launched a survey to crowdsource ideas and suggestions of incidents to look at. The aim of the survey was to get a general idea of what cybersecurity incidents people are interested in and care about. The obtained list of incidents that 'inspire and strike fear' were then narrowed down for deeper analysis.

[9] IGF 2023 BPF Cybersecurity Kick-off call, 2 May 2023, summary at https://www.intgovforum.org/en/filedepot_download/56/25033

On 22 June, the BPF discussed[10] a longlist of incidents[11], categorised on the basis of timeframe, type of incident, geographical impact, and the impact on international stability. BPF participants further reviewed and consolidated the list of 'incidents of interest'. (see table next page)

The BPF then launched a call for volunteers to collaborate on concise analysis of the shortlisted events, based on what is out in the public domain in terms of information, opinions, statements, anecdotal evidence, etc.. The help of people with local knowledge, including non-English language, was seen as important to collect stories reflecting first responder and victim perspectives, e.g. from local newspapers or other local online resources, interviews, etc. .

To structure the analysis it was suggested to look at the impact on 5 sectors or stakeholder groups that are enshrined in many cyber norms agreements, are of particular concern, or can rely on a certain level of protection: people, critical infrastructure/critical information infrastructure, government services, technical infrastructure, the incident's first responders. The description of each incident would then conclude with an analysis of how the incident affected international peace and stability and the relation between states. Summarised, the analysis were expected to answer the following research questions:

1) What was the impact on people?
2) What was the impact on CI/CII?
3) What was the impact on government services?
4) What was the impact on technical (infra)structure?
5) What was the impact on incident responders?
6) How did the incident affect international peace and stability, relations between states?

The analysis of the volunteer groups can be found in the final section of the report.

[10] IGF 2023 BPF Cybersecurity, Virtual meeting 22 June, summary at https://www.intgovforum.org/en/filedepot_download/56/25833

[11] The list of incidents included: the Solarwinds software supply chain attack (2019-2020), the Costa Rica ransomware incidents (2022), the Medibank data breach (2022), various ransomware incidents in the Pacific (2021-2023), DTB Bank Ransomware Tanzania, Notpetya, Bank of Zambia ransomware incident (2022), the BlackAxe online scams (2022-2023), the Colonial Pipeline ransomware incident (2021), venomous vaccines and fake jobs scam campaign targeting Arabic speakers (2022-2023), events targeting elections or key democratic institutions in Estonia and France (2023).

Shortlist of incidents of interest for BPF review - selected to be geographically diverse and diverse in type of incidents

SHORTLIST OF CYBERSECURITY INCIDENTS FOR 2023 IGF BPF ON CYBERSECURITY

Name/case	Costa Rica*	Medibank*	Ransomware Pacific*	BlackAxe*	Colonial Pipeline	Hacking democracies*
Analysis of the incident - how did the incident become known? - what happened with the incident? - what was the response by CERTs, government, and affected entities? - how was the response organised - public-private; national-international ?	*Costa Rican govt agencies fell victim to a ransomware operation which caused international trade, customs operations to come to a standstill. CR declared a state of emergency, and state of war.*	*Medibank, a private health insurance company, suffered a data breach. The hackers threatened to release sensitive personal data in return for a payment. The company refused payment and data was leaked on darknet.*	*Various unrelated incidents affecting PNG Department of Finance, Tonga's Cable Communication, and Vanuatu's e-government portfolio*	*Police arrested more than 70 alleged fraudsters linked to a Nigerian criminal network known as Black Axe in South Africa, Nigeria and Ivory Coast – as well as in Europe, the Middle East, south-east Asia and the US. BlackAxe is held responsible for online scams and running digital extortion schemes.*	*The Colonial Pipeline Company halted all pipeline operations after it suffered a ransomware attack. Overseen by the FBI, the company paid the amount that was asked by the hacker group (75 bitcoin or $4.4 million USD). Upon receipt of the ransom, an IT tool was provided to restore the system but it had a very long processing time to get the system back up in time.*	*Two separate incidents that affected elections or key democratic institutions. Attacks on Estonia's elections; DDoS on France's*

*It was suggested to add the SolarWinds incident to the shortlist and revisit the research that was conducted by the BPF Cybersecurity in 2022.

Observations and key findings

About the 2023 timeframe

The international cyber norm discussions within the UN First Committee rightfully focus their discussions on responsible state behavior. However, when considering the development, application, and impact of these norms, it is useful to understand how they play out in practice and be fully informed of the flow on effect across the wider ecosystem.

This year’s BPF looked at a range of diverse incidents from recent years with the aim to draw linkages between incidents and the international cyber norms discussion, echoing work of previous BPFs, as well as identifying flow on impacts for individuals, particularly across the wider public.

The ambitious scope of this year's BPF stood under pressure for the IGF timeframe with an earlier IGF annual meeting, reducing the time for analysis by roughly two months compared to previous years and making July and August - traditionally months with lower activity - the most important period for the research and analysis. Not all envisaged goals have been met and this year’s BPF work is very much a starting point for wider investigation seeking to ground discussions of international norms in real incidents and inform them on the wider impacts cyber incidents can have on the everyday lives of citizens, regardless of State or non-state involvement.

While the BPF’s work remains preliminary, there are some early themes developing across the cases examined.

Impact of cybersecurity incidents

Discussions around major cyber incidents often revolve around the technical, financial, legal, and intergovernmental consequences. However, the opportunities and challenges presented across the cyber ecosystem ultimately lie with the public, whether individuals or societies affected directly by a cyber incident or through the resonating impacts of an incident.

Across the cases explored several themes can be identified. These include:

- the impact on human services;
- privacy and data concerns;
- the amplification of existing contextual dynamics;

- and notable policy responses.

The impact on human services is relatively clear across most of the cases presented. For example, in Costa Rica (2022), an attack on the servers of the Costa Rican Social Security Fund (CCSS) led to a shut down of all critical systems, which resulted in adverse human impacts including the non-payment of salaries to teachers and a loss of access to patient health records.

The case of Vanuatu (2022), where the government broadband network was impacted follows a similar profile.

Given the time frame of many of the incidents explored, COVID-19 response may have also been affected. This can be seen directly as in the case of Fiji (2021) as well as Costa Rica (2022), and potentially indirectly in other instances due to the effect on government spending, hospital service, and in other areas.

As with any ransomware that includes suspected data exfiltration, there is a concern and potential impact on individual privacy and data. This can be seen most prominently in the case of Medibank (2022) where extremely sensitive customer details, including health records, were stolen by criminal actors.

The amplification of existing contextual dynamics is particularly interesting as these flow-on effects can have a resonating impact well beyond the technical or service delivery space. These include the clear case of Fiji (2021) where the incident fed into pre-existing concerns around COVID-19 misinformation and in Samoa (2021) where lack of clear initial communication led to speculation adding to narratives surrounding the recent election controversy.

Beyond these more direct connections, the impact of incidents do have a flow on impact on the confidence in government, the institutions, businesses, and the use of digital technologies across the board with potential long term reverberations. This can be seen more immediately when exploring the impact of communication approaches around an incident, with more proactive and clear communications often mitigating additional potential negative outcomes.

Together, any of these incidents alongside other cyber related developments have seen a relatively strong policy response, with decision makers increasingly aware of the importance of the space and policy and investment reflecting this.

For SolarWinds, the working groups found the impact of the incident is reflected across U.S. government and European Union policy, guideline, norm, regulation, and guidance documents related to cybersecurity and the creation of the Cyber Safety Review Board (CSRB). In the case of Black Axe, clear cybercrime legislation and collaborative agreements can be counted in the aftermath. For the Pacific, the recent Lagatoi Declaration as well as new policy initiatives, investment in existing or development of new incident response teams, and other positive trends.

Normative Links

Regardless of any attribution in the cases examined, there are clear norms that could be directly applied to prevent, respond, or mitigate the impacts of the incidents explored. Discussion around the impact the UN GGE norms have or could potentially have in real incidents is an important area to explore, one that the BPF has looked into in the past.

These can include the importance of ensuring supply chain security as highlighted in the Solarwind Breach case (2020); do not damage critical infrastructure and protect critical infrastructure as arguably applicable in the cases of ransomware targeting government systems in Papua New Guinea (2021), Costa Rica (2022), Vanuatu (2022) and others; and respecting human rights and privacy as seen across incidents involving exfiltration of data, for example during the Medibank case (2022) explored.

With the cases this year, there are key norms that can be seen in action. This is not to say the activity was driven consciously by norms, but that the spirit captured by the norm was applied in practice.

Unsurprisingly, those seen across the case studies examined include:

- Interstate cooperation on security;
- Respect for human rights;
- Cooperate to stop crime and terrorism;
- Respond to requests for assistance;
- Report ICT vulnerabilities;
- And the importance of cyber capacity building.

Interstate cooperation on security and responding to requests for assistance are key elements in the incident response around many of these cases. In particular this can be seen in the example of Costa Rica in 2022, where assistance was sought from other countries including the US, Spain and Israel.

Similar collaboration can be seen across the ransomware incidents in the Pacific where, when requested, interstate information sharing and active incident response support was provided in many of the cases.

Cooperation to stop crime and terrorism is particularly highlighted in the case of the Black Axe cyber incidents where both the cybercrime activities conducted by the Black Axe group as well as the physical crimes, including trafficking, both involved cross border elements and law enforcement cooperation.

Report ICT vulnerabilities is a critical part of mitigating the potential impact of vulnerabilities and most prominently featured in the case of Solar Winds. While 18,000 Solarwinds customers did install the malicious updates, early reporting, initially by FireEye, did help initiate response and assist in mitigating even further impacts of the vulnerability.

The relevance of the human rights norm also underpins many of the cases studied. Attacks on critical services, such as in the Costa Rica case, impair access to services which impact human rights, including the right to education and health care. Data exfiltration will also undermine the right to privacy and the protection of personal data, and the exfiltration of particularly sensitive data can also result in discriminatory impacts on the basis of protected characteristics.

Cyber capacity building is the most prominent theme across the incidents explored, with the need for further cyber capacity building activities made clear and in many cases acted upon. More significantly however, many of the incidents explored showcased the positive impact cyber capacity building activities had on economy's and organization's ability to respond to the incidents themselves. For example in the cases of ransomware impacting the Pacific, the extensive efforts to develop national incident response capability and collaborative networks across the region helped to facilitate information sharing and active collaborative incident response.

The initial findings of the case study working groups can be found in the next section. The hope is that the work can continue through the next phase of IGF BPF-Cybersecurity.

Cases Explored

I. Black Axe cyber incidents

Text based on the analysis by BPF volunteers Eleanor Sarpong, Helena Huang Yixin, et al.

Description

Event: The Cape Town Zone Black Axe Prosecutions

Press release:

Eight Nigerians Charged with Conspiring to Engage in Internet Scams and Money Laundering from Cape Town, South Africa

Court documents:

https://www.justice.gov/media/1172661/dl?inline
https://www.justice.gov/media/1172666/dl?inline

Current status (as of 7 Jun):

“The courts are still arguing the technicalities of whether South Africa can indeed hand them over to US authorities.“ , “In a nutshell, the argument revolved around how the co urt should decide if they should be extradited, and the processes that should be followed in terms of the Extradition Act and the treaty between South Africa and the US.“

https://www.news24.com/news24/southafrica/news/alleged-black-axe-scammers-challenging-extradition-to-us-20230607

Types of crimes and Modus Operandi (lifted from US DOJ’s press release)

Types of crimes:

Internet fraud involving romance scams and advance fee schemes

Modus Operandi:

Many of these fraudulent narratives involved claims that an individual was travelling to South Africa for work and needed money or other items of value following a series of unfortunate and unforeseen events, often involving a construction site or problems with a crane. The conspirators used social media websites, online dating websites, and voice over internet protocol phone numbers to find and talk with victims in the United States, while using a number of aliases.

The conspirators’ romance scam victims believed they were in romantic relationships with the person using the alias and, when requested, the victims sent money and items of value overseas, including to South Africa. Sometimes, when victims expressed hesitation in sending money, the conspirators used manipulative tactics to coerce the payments, including by threatening to distribute personally sensitive photographs of the victim.

The conspirators used the bank accounts of victims and individuals with U.S.-based financial accounts to transfer the money to South Africa. On certain occasions, the conspirators convinced victims to open financial accounts in the United States that the conspirators would then be permitted to use themselves. In addition to laundering money derived from romance scams and advance fee schemes, the conspirators also worked to launder money from business email compromise schemes. In addition to their aliases, the conspirators used business entities to conceal and disguise the illegal nature of the funds.

Otubu also engaged in romance scams and used the victims of those scams to obtain money and to launder the proceeds of business email compromises back to South Africa. Otubu conspired with an individual identified in the criminal complaint as Co-conspirator 1, who was a founding member and leader of the Cape Town Zone of Black Axe.

Other similar incidents

Not related to financial crimes. It appears that the BlackAxe group plays an active role in trafficking women from Benin City to different parts of Europe for sexual services. These European countries include Italy, Spain, France, and increasingly, Switzerland (end 2022-current). However, I've yet to come across information explicitly stating that BlackAxe had recruited these women online, which would then fall under cybercrime. Cocaine sold in Switzerland, reportedly originating in Latin America and West Africa, is sold on the internet by syndicates. There might be strategic interest for the syndicate to be interested in Switzerland due to the banking regulations there which sometimes facilitate money laundering.

- https://www.interpol.int/content/download/15525/file/Online%20African%20Organized%20Crime%20from%20Surface%20to%20Darkweb.pdf#page24
- https://tribuneonlineng.com/eiye-black-axe-cult-groups-run-prostitution-rings-italy-spain/
- https://ocindex.net/country/switzerland

- https://www.swissinfo.ch/eng/society/report--nigerian-black-axe-criminal-gang-expands-in-switzerland/48144916

Observations

Policy-wise, it might have opened up conversations on cybercrime criminals and extradition.
Although this is not explicitly attributed to Black Axe, South African Justice Minister Ronald Lamola and French Foreign Minister Catherine Colonna signed a cybercrime protocol deal in mid-2023. Under the agreement, “South Africa’s prosecutors, the Special Investigating Unit, will gain French training in combating cybercrime. The deal also calls for setting up an anti-cybercrime academy to train police personnel from South Africa and nearby African countries. “
https://www.theafricareport.com/313729/south-africa-cyber-deal-with-france-hints-at-crackdown-on-computer-criminals/

Key takeaways

-> Importance of partnerships

- Mapping out cases and footprints and timely sharing of information
- Resourcing of key organizations and upskilling of security services in emerging cybersecurity threats.
- Supporting local law enforcements with up to date resources
- Protection of victims post trauma and how to safeguard against future attacks

-> Cybercrime organisations part of larger organisations (some active before turning to cyber crime).

-> best practices/solutions for particular types of cybercrime should not be looked at in silos and such a syndicate perhaps rarely involve themselves in only one type of crime/cybercrime.

-> the fact that there are hardly much information on best practices related to this scope/domain reinforces the need to come up with best practices, and the need for institutions exploring best practices to not only focus on reports but also hear the victim’s side of the story to understand the issue more holistically, in order to come up with policy recommendations that can tackle the issues (more) effectively.

II. Costa Rica incidents

Text based on the analysis by BPF volunteers Ellie McDonald, Nestor Boniche, et al.

Description

Timeline of events: The first wave of ransomware attacks started in April 2022. The second was launched on 31 May 2022. The alleged perpetrator of the first wave of attacks is the ‘Conti’ Group, while the second is believed to have been conducted by the ‘Hive’ Group. Both groups are reportedly based in the Russian Federation.

The first wave of attacks was directed at the servers of the Costa Rican Ministry of Finance, disabling the Virtual Tax Administration (ATV) and the Customs Information System (TICA). Two days later, the website of the Ministry of Science, Innovation, Technology and Telecommunications was defaced. Hours later, Conti attacked an email server of the National Meteorological Institute stealing the information therein.[12] The Conti group claimed responsibility for the first group of attacks and demanded a US $20 million ransom in exchange for not releasing information stolen from the Ministry of Finance, including citizens’ tax returns and sensitive information about companies operating in Costa Rica.[13]

In May 2022, a second attack was launched against the Costa Rican Social Security Fund (CCSS). This forced the CCSS to shut down all its critical systems, including the Single Digital Health Record (EDUS) and the Centralized Collection System (SICERE).[14] The Hive Group allegedly requested a payment of US $5 million in bitcoin, after which it would restore the operations of the CCSS.[15]

[12] Christine Murry & Mehul Srivastava, ‘How Conti ransomware group crippled Costa Rica — then fell apart’, (Financial Times, 9 July 2022). How Conti ransomware group crippled Costa Rica — then fell apart | Financial Times (ft.com).

[13] Associated Press, ‘Costa Rica, 'under assault' is a troubling test case on ransomware attacks’ (NBC News, 17 June 2022). Costa Rica, 'under assault' is a troubling test case on ransomware attacks (nbcnews.com).

[14] Twitter thread of the Costa Rican Ministry of Finance of 19 April 2022 (announcing that, due to the shutdown of the systems, the deadline for filing taxes would be postponed). Costa Rica ransomware attack (2022) - International cyber law: interactive toolkit (ccdcoe.org).

[15] Pratim Milton Datta & Thomas Acton, ‘Ransomware and Costa Rica’s National Emergency: A Defense Framework and Teaching Case’ (2023) Journal of Information Technology Teaching Cases 1. Ransomware and Costa Rica’s national emergency: A defense framework and teaching case - Pratim Milton Datta, Thomas Acton, 2022 (sagepub.com).

The government refused to pay the hackers, labeling them as “terrorist groups”.[16]

Impact: The effects of the attack are reported to have continued for several months until the end of June 2022. The government was forced to temporarily shut down computer systems used to declare taxes and the control and management of imports and exports, causing an economic loss of about US$ 125 million in the first 48 hours following the attack.[17] Teachers were unable to receive paychecks. Health officials were unable to access medical records which impacted patients. The inability to access health records also prevented them from tracking the spread of Covid-19.

Post event response: On 8 May 2022, the president of Costa Rica issued an executive order proclaiming a national emergency due to the cyberattacks against the country’s public sector and stated that the country was in a “state of war”. At the onset of the first wave of attacks, the newly installed President Chaves Robles declared a state of emergency, stating “we’re at war and this is not an exaggeration”.

The government sought assistance from other countries, including the US, Spain and Israel. It was reported that the US provided some technical assistance to Costa Rica through its Cybersecurity and Infrastructure Security Agency as a result of an information-sharing program with nations around the world. The US State Department also offered a reward for the arrest of members of Conti.[18] The Associated Press reported that the situation had “raised questions about the United States’ role in protecting friendly nations from cyberattacks when Russian-based criminal gangs are targeting less developed countries in ways that could have major global repercussions.”[19]

A number of prominent companies provided assistance to the government following the attack. In this early period, the media published the names of these companies, and these companies were in turn subject to cyber attacks.

[16] Joe Tidy, ‘President Rodrigo Chaves says Costa Rica is at war with Conti hackers’ (BBC, 18 May 2022). President Rodrigo Chaves says Costa Rica is at war with Conti hackers - BBC News.

[17] Chamber of Foreign Trade of Costa Rica, ‘$125 millones en pérdidas estima Cámara de Comercio Exterior tras ciberataque que afectó aduanas’ (Facebook post, 19 April 2022). https://www.ameli... - Crecex - Cámara de Comercio Exterior CR | Facebook.

[18] Associated Press, ‘Costa Rica, 'under assault' is a troubling test case on ransomware attacks’ (NBC News, 17 June 2022). Costa Rica, 'under assault' is a troubling test case on ransomware attacks (nbcnews.com).

[19] Alan Suderman & Ben Fox, ‘Costa Rica chaos a warning that ransomware threat remains’ (AP News, 17 June 2022). Costa Rica chaos a warning that ransomware threat remains | AP News.

The trade unions negotiated with the government to ensure workers were paid despite the shutdown of the social security computer systems.[20]

Observations

The case demonstrated the importance of norms (f), (g) and (h) relating to the protection of critical infrastructure: the ransomware attacks led to the suspension of critical infrastructure, including health services and social security systems responsible for the payment of salaries.

The relevance of the norm (e) relating to respect for human rights is also evident. Attacks on critical infrastructure impair access to services which impact human rights, including the right to education and health care. Data exfiltration will also undermine the right to privacy and the protection of personal data, and the exfiltration of particularly sensitive data can also result in discriminatory impacts on the basis of protected characteristics.

Norms (i) and (j) relating to ensuring the integrity of the supply chain and the reporting of ICT vulnerabilities were also implicated, as the attacks demonstrated the vulnerabilities of the government's data infrastructure.

Norm (d) relating to interstate cooperation is relevant given the support received from the US.

Key takeaways

Key highlights of and reflections on the incident

The ransomware attacks demonstrate where a law enforcement issue becomes one which imperils national and human security. The attacks caused significant disruption, impacting the government's ability to collect tax and custom revenues and to deliver critical services. It also had significant human impacts, disrupting access to healthcare services and the payment of salaries.

Impact on human services: The Ministry of Finance, including tax and customs services, and social security services, including health records were all impacted, causing

[20] Office of the President of Costa Rica, 'Conferencia de prensa del sector educativo - 21 de mayo 2022' (Facebook, 21 May 2022) (confirming that the government has signed an agreement to advance the payment of the 3'160 teachers who were unable to receive paychecks due to the shutdown of the systems). Conferencia de prensa del sector educativo - 21 de mayo 2022 | Conferencia de prensa del sector educativo - 21 de mayo 2022 | By Presidencia de la República | Facebook.

an economic loss of about US$ 125 million in the first 48 hours following the attack.[21] It is possible to extrapolate the overall economic loss during the attacks, which affected the government for a period of several months up until June 2022. This economic loss is likely to impact the provision of public services and other goods which will in turn have a tangible human impact as reduction in government spending is more likely to impact those who are the most reliant on such services, including persons with disabilities, women during maternity, etc.

The country's COVID-19 response was adversely affected, as health records, including the Single Digital Health Record (EDUS) and the Centralized Collection System (SICERE), were temporarily inaccessible. This was particularly critical given the global context of the Covid-19 pandemic and the need to track exposure to the virus.

The attack on the Costa Rican Social Security Fund (CCSS), which forced the CCSS to shut down all its critical systems, including the Single Digital Health Record (EDUS) and the Centralized Collection System (SICERE), impacted the payment of salaries to teachers.

Privacy and data concerns: Following the government's refusal to pay the ransom, Conti posted victims' files on its dark web site. This impacted all those whose sensitive data was compromised. Even to this day, many individuals and companies are not aware if the data was exfiltrated or published.

Role of external Actors: The attack demonstrated the need for a collective and coordinated approach which is inclusive of different stakeholders.

Assistance was sought from other countries including the US, Spain and Israel. It was reported that the US provided some technical assistance to Costa Rica through its Cybersecurity and Infrastructure Security Agency as a result of an information-sharing program with nations around the world.

It is also important to recognise the role of other private and public actors, including companies and others that provided assistance.Companies who provided assistance to the government were later reported to become the object of cyber attacks.

[21] Chamber of Foreign Trade of Costa Rica, '$125 millones en pérdidas estima Cámara de Comercio Exterior tras ciberataque que afectó aduanas' (Facebook post, 19 April 2022). https://www.ameli... - Crecex - Cámara de Comercio Exterior CR | Facebook.

III. Medibank incident

Text based on the analysis by BPF volunteers Ying Chu Chen, Bart Hogeveen, et al.

Description & Observations

Medibank Private (Medibank, the company) is an Australian health insurance company. It provides private health insurance and health services to Australian people.

The company announced it had been compromised by a malicious actor resulting in the theft of over 200 GB of customer data. The actor released 100 policy records on the Darkweb from Medibank's Australian Health Management (AHM) and international student systems as a sample to potential buyers. Personal data included in the files covered the name, date of birth, address, phone number and email address of around 9.7 million current and former customers and some of their authorised representatives. This figure represents about 5.1 million Medibank customers, approximately 2.8 million AHM customers and about 1.8 million international customers. The stolen data also included additional sensitive information such as the location where a customer received medical services and insurance codes relating to their diagnosis, treatment and procedures.

Whilst investigating the incident, medibank continued to work closely with the government and regulators and keep their customers updated with periodic press releases and direct customer communications.

Two months later, on December 1, 2022, the Office of the Australian Information Commissioner (OAIC) announced an investigation into the Medibank data breach incident. The OAIC's investigation focused on the incident, Medibank's control effectiveness and response to the data loss. OAIC found the company contravened Australian privacy law, enabling the Commissioner to seek civil penalties up to AUD 2.2 million (USD 1.47 million) through the Federal Court for each infringement.

Medibank disclosed that a criminal used a stolen username and password from a third-party service provider to access Medibank's system. The criminal then accessed the company's internal network through a misconfigured firewall which did not require an additional security certificate. The criminal then moved laterally across the network by gathering additional usernames and passwords to access further internal databases without the need for authentication. [22]

Medibank acknowledged that the data loss would likely cause distress for its customer base but reassured that the stolen data would likely not be sufficient to enable financial fraud. During the incident review responders discovered that much of the data was incomplete or challenging to understand. After the investigation, Medibank concluded that the criminal did not access primary identity documents. The company provided some helplines and support programs.

The Australian Prudential and Regulation Authority (APRA) said the Medibank incident in October 2022 was Australia's most significant data breach event and asked Medibank to provide remedy measures in June 2023. APRA asked Medibank to increase their capital adequacy requirement of AUD 250 million. Medibank says the company will comply with the requirements of APRA. Medibank also announced that they would defer premium increases for all Medibank and ahm customers for three months.

The Medibank case is not the only data breach incident in the Asia Pacific area, e.g., Singapore had a SingHealth data breach in 2018, Malaysia had a data leak from a private entity in 2019, and Taiwan and Japan also had an identity data leak incident in 2023. These types of data breach incidents continue to test the capabilities of government and private sector orgainsations. They must prevent harmful behaviour, such as identity fraud, to their citizens. People in those economies also need to be aware of how to protect themselves to prevent fraud or any harmful behaviour that causes their loss of property or health.

Timeline:

- Medibank Private Cyber Security Incident

References:

1. Medibank cyber incident response
2. OAIC opens investigation into Medibank over data breach
3. Medibank cybercrime update
4. APRA takes action against Medibank Private in relation to cyber incident
5. Medibank response to APRA announcement

[22] Medibank Cyber event timeline, https://www.medibank.com.au/health-insurance/info/cyber-security/timeline/ (23 February, 2023)

Key takeaways

Medibank quickly disclosed the incident to the Australian Stock Exchange and contacted their customers about the incident. Medibank was transparent throughout the investigation and remediation process and published an incident timeline on their public website. They also posted a summary of their findings and an outline for how they will work to increase their security posture and resilience. Regulators also commissioned an independent third-party review into the incident to understand the breach, any control failures and to clarify obligations and improvements moving forward.

Third party and supply chain risk continues to present a significant challenge to organisational security. Many data breaches stem from third-parties that are not sufficiently integrated into an organisation's holistic security posture.

Data theft motivated by identity fraud and financial crime is an ongoing and serious issue. The theft of extremely private and sensitive health information is a crime that impacts communities and the public in new, and potentially more distressing ways. It is essential that in such incidents effective support channels for victims are created that encompass financial impacts - but also any emotional distress, such as mental health support services.

IV. Pacific ransomware incidents

Text based on the analysis by BPF volunteers Eugene Tan, Cherie Lagakali, et al.

Description

With increased connectivity, a focus on digital transformation, and the widespread adoption of social media across the Pacific, has increased the prevalence and reliance on digital systems across government, business, and society. As in any other region, the Pacific has seen a rise in the number and sophistication of scams and cybercrimes, challenges around misinformation online, and numerous other cybersecurity challenges. One particular trend of note has been the increase in publicly reported ransomware attacks against Pacific government systems and critical infrastructure. A few examples of recent publicly reported incidents include:

- **April 2021** ransomware impacting Fiji’s government network GovNet linked to Sodinokibi (REvil)

- **August 2021** ransomware impacting computers at Samoa's Ministry of Works, Transport, and Infrastructure (MWTI)
- **October 2021** ransomware impacting the Papua New Guinea Ministry of Finance linked to HIVE ransomware
- **November 2022** ransomware impacting the Vanuatu government network linked to RansomHouse
- **February 2023** ransomware impacting the Tonga Communications Corporation (TCC) linked with MedusaLocker ransomware

While these do not constitute the entirety of publicly reported incidents in the region and certainly not the extent of all incidents impacting Pacific networks, they do show an interesting cross section of the impact of ransomware on government networks as well as the development of the region's response.

Observations

April 2021, Fiji

In April 2021, the Fiji government announced that the Government ITC Department was managing a cyber incident targeting the government network. The source of the incident was revealed to be from a separate department, however government services were disrupted as a part of precautions associated with the response.

The impact on government services resulted in COVID vaccination registration systems being down for a few days. Medical teams were out on field with tablets, registering the local communities and then vaccinating when they experienced problems verifying birth registration details. It was Fiji's second round of the virus and Fiji's second largest hospital in the western division was also on lockdown due to hospital staff and patients catching COVID. At first the medical teams thought that they had internet problems. It was later thought that the vaccination registration system which had at the time just been rolled out, had bugs in it and had not been properly tested. The nation's birth registration system was being used to identify and verify individuals before the medical system was updated and they could get vaccinated. Data was being pulled through two different systems, one from registry, one from medical and then the vaccination approval before the system was updated and the individual was vaccinated. While this might have seemed like a flawless process in the urban centres with faster internet, most parts of Fiji particularly in the villages and remote areas that still run on solar, require one to stand still at a particular spot aligning with the telecom towers for proper internet. This was at a time where there was widespread distrust of the vaccines and women were required to re-register with their maiden names as part of the vaccination process. Later, it was announced that there was an incident and that government teams were investigating it.

The incident received media attention in Fiji and has been linked to the threat actors Sodinokibi (REvil).

Select sources:
https://www.fiji.gov.fj/Media-Centre/News/STATEMENT-FROM-THE-ATTORNEY-GENERAL-AND-MINIST-(3)
https://www.fijitimes.com/cyber-attack-disrupts-state-online-services/
https://www.databreaches.net/fj-cyber-attack-disrupts-government-online-services/

August 2021, Samoa
From 2 to 3 August 2021, the Samoa Ministry of Works, Transport, and Infrastructure (MWTI) identified a ransomware attack impacting eight computers. While the extent of the impact was limited to the eight computers and the extent of the damage was seen as non-critical infrastructure, the loss of data on these systems, the timing of the attack shortly after a contentious election, and early media reporting with delayed public statements by the government led to wide speculation. These included inaccurate speculation on the extent of the impact and accusations that the previous government has wiped the systems.

As compared to the Fiji incident, the government's public communications were more detailed, however, these were seen to have been in response to media reporting rather than as a proactive measure.

Select sources:

- https://www.samoagovt.ws/2021/08/ransomware-cyber-attack-on-m-w-t-i-clarification/
- https://www.samoaobserver.ws/category/samoa/89934
- https://www.samoaobserver.ws/category/samoa/89768
- Stories from the Pacific - the human side of cyber incidents. 30 August 2023. Session at the APrIGF, Brisbane, AU

October 2021, Papua New Guinea

On 22 October 2021, the Papua New Guinea Department of Finance detected a ransomware infiltration impacting the Department's Integrated Financial Management System (IFMS). The attackers demanded payment in bitcoins for restoration of services. This attack impacted the ability of the government to make payments, carry out basic functions,and access foreign aid.

By 29 October, the Minister of Finance confirmed that the Financial Management System had been fully restored, however lingering challenges did see the impact of the incident extend further with transactions requiring the use of a controlled environment and paper transactions. This included reported flow on impacts from the delay of the PNG budget, impacts for local government and COVID-19 response associated with the pause in payments and delayed budget.

Government communications around the event were relatively comprehensive, including statements sharing that the ransomware was identified to have similar characteristics to HIVE ransomware.

Select sources:

- https://www.rnz.co.nz/international/pacific-news/454467/png-government-system-hit-by-ransomware-attack
- https://www.forumsec.org/wp-content/uploads/2023/01/Pacific-Security-Outlook-Report-2022-2023.pdf
- https://securityaffairs.com/123927/cyber-crime/papua-new-guinea-ransomware.html
- https://informationsecuritybuzz.com/papa-new-guineas-finance-department-suffers-massive-ransomware-attack/
- https://www.securityweek.com/ransomware-attack-hits-png-finance-ministry/
- https://twitter.com/cloudpng/status/1455081004691955714?s=20
- https://news.pngfacts.com/2021/11/cyber-attacks-escalating-ict-to.html
- https://news.pngfacts.com/2021/10/png-government-financial-system-fully.html
- https://twitter.com/sasindranpng/status/1455421571212865537/photo/1
- https://www.fijivillage.com/news/PNG-delays-budget-as-cyber-attack-woes-continue-8r54fx/

November 2022, Vanuatu

The Vanuatu Government Office of the CIO and CERT VU detected suspicious activity within the Vanuatu Government Broadband network (GBN). This activity escalated to a ransomware incident that compromised the GBN, impacting all government online services, including government email, network file sharing, VoIP, financial systems, and other critical services. RansomHouse added the Government of Vanuatu to their leak site on December 24.

Given the scale of impacted services, the recovery of services was over a long period of time, with reports of pen and paper being used in the hospital system in November, 70% recovery of services in December, and months of lost court data reported in January.

Government response to the incident was comprehensive and communications around the incident have been extensive. Communications have included sharing of lessons learned from the response effort, including on the sidelines of the UN OEWG.

Select sources:

- https://www.dailypost.vu/news/70-of-government-servers-recovered-pm-kalsakau/article_5d1b4ade-43e5-50a0-9a42-f6b8e5c63b46.html
- https://www.rnz.co.nz/international/pacific-news/479936/most-government-servers-back-on-after-cyber-attack-says-vanuatu-pm
- https://www.bbc.com/news/world-asia-63632129
- https://www.dailypost.vu/news/5-months-worth-of-court-data-lost-in-ransomware-attack/article_2b41aad2-14a6-5e46-b2a0-d5b9bf26bf7a.html
- https://www.dailypost.vu/news/government-will-not-stoop-down-to-hackers/article_29697cf5-ca7d-578c-b930-c36164d2373d.html
- https://techmonitor.ai/focus/vanuatu-is-showing-small-nations-how-to-resist-big-cyberattacks
- https://www.dailypost.vu/news/ransomhouse-claims-attack-on-vanuatu-government-network/article_60e99298-1b39-5066-a282-5808b95bd7df.html
- https://www.abc.net.au/news/2022-11-29/cyber-hack-cripples-vanuatu-public-sector/101705322
- https://rusi.org/explore-our-research/publications/conference-reports/decoding-emerging-threats-ransomware-and-prevention-future-cyber-crises

February 2023, Tonga

On 14 February 2023, ransomware encrypted a portion of the systems of the state-owned telecommunication company Tonga Communications Corporation (TCC).

The ransomware affected corporate systems, impacting connecting new customers, billing, and managing customer enquiries, while delivery of voice and Internet services was reported to be unimpacted.

TCC accounts for around 70% of the market share of dial-up and broadband Internet in the country and manages more than half the population's mobile services. Response took place within three days with researchers pointing to the Medusa ransomware group as claiming the attack.

Select sources:

- https://therecord.media/tonga-is-the-latest-pacific-island-nation-hit-with-ransomware
- https://izoologic.com/2023/03/01/tonga-communications-corporation-suffered-a-ransomware-attack/
- https://www.facebook.com/photo?fbid=518654497083534&set=a.504685261813791
- Stories from the Pacific - the human side of cyber incidents. 30 August 2023. Session at the APrIGF, Brisbane, AU

Key takeaways

Across all the examples explored there are a few common threads found in the impact of these incidents on responders and individuals. These include the impact on human services; privacy and data concerns; the amplification of existing contextual dynamics; the role of external partners; and notable policy responses.

The impact on human services is relatively clear, with services to the public impacted in all listed cases. This impact is both direct as in the case of Vanuatu and indirect in the case of Papua New Guinea, where the impact on payments and finance had a flow on impact on the delivery of government services, and in Tonga where the impact in corporate systems could effect business operations, despite continued service delivery. Given the time frame of the incidents, COVID-19 response was also affected directly as in the case of Fiji and potentially indirectly in other instances due to the effect on government spending, hospital service, and in other areas.

As with any ransomware that includes suspected data exfiltration, there is a concern and potential impact on individual privacy and data concerns. This likely played a part in all the listed cases.

The amplification of existing contextual dynamics is particularly interesting as these flow-on effects can have a resonating impact well beyond the technical or service delivery space. These include the clear case of Fiji where the incident fed into pre existing concerns around COVID-19 misinformation and in Samoa where lack of clear initial communication led to speculation adding to narratives surrounding the recent election controversy.

In a more positive trend, the role of external partners also has a key role to play, particularly for incident responders. In nearly every incident, there is a public acknowledgement of government and/or private sector support provided in the response and recovery from these incidents. These show the importance of building strong collaborative and trusted networks as well as the value of cyber capacity building

Together, these incidents alongside other cyber related developments have seen a relatively strong policy response, with decision makers increasingly aware of the importance of the space and policy and investment reflecting this. This includes the recent Lagatoi Declaration as well as new policy initiatives, investment in existing or development of new incident response teams, and other positive trends. There are signs of growing capability for response in the Pacific, strong efforts towards raising public awareness, and dynamic regional collaboration for incident response. There are also signs of more open and proactive approaches to incident response communications across the region.

The UN Norms of Responsible State Behavior in Cyberspace Most Impacted include:

- 1 - Interstate Cooperation on Security
- 8 - Respond to Requests for Assistance
- The need for and value of cyber capacity building initiatives

V. Solarwinds Breach (2020)

Text based on the analysis by BPF volunteers Allison Wylde, Dino Cataldo Dell'Accio, et al.

Description[23]

The SolarWinds breach occurred as part of a routine update for its Orion IT software. As with other client software, Orion was designed to download updates. A custom-made backdoor program then enabled attackers to gain access to the SAML and add malicious payload. The breach, named Sunburst, was installed during routine updates, initiating the compromise. The program was hidden in legitimate software to appear as though it was a telemetry sending program. The program did not execute immediately. It was designed to evade antivirus (AV) protection and sandboxes. It tried to identify what monitoring or management software was running or blocking.

Sunburst was designed to provide the attackers with information about the entity through sending encoded DNS requests to the C&C server. The initial attack targeted more than 18,000 users with the attackers carefully selecting 100 entities for a deeper second stage attack. The actual time line was found to have started with secondary attacks in April 2020. The breach targeted confidential information belonging to multiple government agencies, organizations including the financial sector, universities and medical institutions, and cybersecurity companies. Victims included 425 of the US Fortune 500, the top ten US telecommunications companies, the top five US accounting firms, all branches of the US Military, the Pentagon, the State Department, as well as hundreds of universities and colleges worldwide. The second stage attack carefully extracted further targeted material. The sensitivity of the breach may mean that the full extent of this breach may never be publicly released and may be restricted to the international intelligence community.

Observations

The original contributors providing the Solarwinds analysis as part of the BPF 2021 work, Fred Hansen, Barbara Marchiore de Assis and Allison Wylde (team-leader) undertook qualitative, inductive research with a purposive sample of 3 cyber security experts. In-depth interviews with fixed questions were used: Describe the incident and your role; What do cyber norms mean to you?; What cyber norms do you think apply in this case?; What cyber norms do you think have been, or would have been, helpful in this case?;

[23] Description based on the BPF Cybersecurity report from 2021.
IGF 2021, Best Practice Forum Cybersecurity, '*The Use of Norms to foster Trust and Security.*' p. 67-70.
https://www.intgovforum.org/en/filedepot_download/235/20623

What cyber norms did you, or might you hope to, see arising from this case?), then a thematic analysis to draw out the most important themes. Research ethics were approved through Cardiff University Ethics Research Committee (UREIC 2021).

Cyber norms identified included norm violations, norms 1., the non interference of the public core of the internet and 8., offensive cyber operations by non-state actors (https://hcss.nl/gcsc-norms/).

Norms identified that could have been helpful: Attribution; Financial sanctions/ Company and personnel sanctions; Implementing enhanced cybersecurity; Implementing increased cooperation and policy at the level of nation states - suggest revisit and stress = cooperation, to build trust, (build, promote trust - consistent with the recommendations of the BPF 2021, WORKSTREAM 1)

Policy subsequently implemented

The **United States government** has issued several policy, guideline, norm, regulation, and guidance documents related to cybersecurity since the SolarWinds breach.
Some examples include:

1. White House Fact Sheet (2022) on Advancing Zero Trust Architecture - This fact sheet describes the zero trust architecture concept and its potential benefits for reducing cyber risks. It provides recommendations for implementing zero trust principles within federal agencies and the broader public and private sectors. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
2. White House Fact Sheet (2023): Fact Sheet Biden-Harris National Cybersecurity Strategy:

    Pillar ONE, DEFEND CRITICAL INFRASTRUCTURE;
    Pillar TWO, DISRUPT AND DISMANTLE THREAT ACTORS;
    Pillar THREE, SHAPE MARKET FORCES TO DRIVE SECURITY AND RESILIENCE;
    Pillar FOUR, INVEST IN A RESILIENT FUTURE;
    Pillar FIVE, FORGE INTERNATIONAL PARTNERSHIPS TO PURSUE SHARED GOALS.
    https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

On 30 October 2023, the **US Security and Exchange Commission (SEC)** announced charges against the CISO of the SolarWinds company.
https://nationalcioreview.com/articles-insights/information-security/breaking-feds-take-unprecedented-action-against-ciso-in-solarwinds-case
SEC Press release: https://www.sec.gov/news/press-release/2023-227

The **European Union** has issued several policy updates and recommendations related to cybersecurity in response to the SolarWinds hacking incident; including:

1. Recommendation from the European Commission on strengthening network security and resilience against cyberattacks (COM(2021) 35 final).
   This recommends measures such as improving threat detection capabilities, enhancing information sharing between Member States, and increasing cooperation with third countries.
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0359
2. Updated version of the NIS Directive (Directive (EU) 2016/1148), which includes provisions aimed at preventing and mitigating cyber threats.
   http://data.consilium.europa.eu/doc/document/ST-11000-2020-INIT/en/pdf
3. Recommendations from ENISA (the European Union Agency for Cybersecurity) on improving cybersecurity practices across various sectors, including critical infrastructure and supply chains.
   https://www.enisa.europa.eu/topics/threat-risk-management/guides-and-good-practices/cybersecurity-best-practice-guides
4. Guidance from the European Data Protection Board (EDPB) on data protection implications of the SolarWinds attack.
   https://edpb.europa.eu/sites/default/files/files/file1/edpb_-_solarwinds_statement_en.pdf
5. A joint statement from the European Parliament and Council on the need for increased cybersecurity investments and cooperation among Member States.
   https://www.europarl.europa.eu/doceo/document/TA-9-2021-0000_EN.html

Analysis by a National Audit Office. In January 2022, the US Government Accountability Office) (GAO recognized that the recent cybersecurity incidents (i.e., SolarWinds and the zero-day Microsoft Exchange Server), presented significant cyber threats. The GAO noted that according to the Cybersecurity and Infrastructure Security Agency (CISA), the potential exploitation from both incidents posed an unacceptable risk to federal civilian executive branch agencies because of the likelihood of vulnerabilities being exploited and the prevalence of affected software.

In accordance with the GAO report (https://www.gao.gov/assets/gao-22-104746-highlights.pdf) GAO performed its work under the authority of the Comptroller General to conduct an examination of these cybersecurity incidents in light of widespread congressional interest in this area.

Specifically, GAO's objectives were to (1) summarize the SolarWinds and Microsoft Exchange cybersecurity incidents, (2) determine the steps federal agencies have taken to coordinate and respond to the incidents, and (3) identify lessons federal agencies have learned from the incidents; and Identified the following lessons learned:

(i) Coordinating with the private sector led to greater efficiencies in agency incident response efforts;
(ii) Providing a centralized forum for interagency and private sector discussions led to improved coordination among agencies and with the private sector;
(iii) Sharing of information among agencies was often slow, difficult, and time consuming; collecting evidence was limited due to varying levels of data preservation at agencies.

Key takeaways

From our research the following key points have emerged:

- policy measures, recommendations and lessons learned: the policy action zero trust is now implemented and
- goals for cooperation, coordination and capacity-building are recommended.

Summary of the BPF session at IGF 2023

12 October 2023, Kyoto Japan

Session details

Introductory notes

Ms Hariniombonana Andriamampionona (MAG Liaison)
Mr Wim Degezelle (IGF Consultant)
Mr Klée Aiken (FIRST, BPF co-facilitator

Panel discussion: ‘Exploring cyber incidents, norms, and the impacts at human level’

Ms Louise Marie Hurel (RUSI)
Mr Dino Cataldo Dell’Accio (UNJSPF)
Ms Susan Garae (GFCE Pacific Hub)
Mr Kivuva Mwendwa (KICTAnet)
Moderator: Mr Klée Aiken

O&A with the audience

Session recordings https://youtu.be/Ow20fycVx_A
(available in Arabic, Chinese, English, French, Russian, Spanish, Japanese)

Summary & discussion highlights

- Bridging the gap between the more technical environments and the diplomatic environments will allow to learn from real life experiences with cyber incidents.

- Countries from different regions may understand ‘responsibility’ and ‘responsible behaviour’ differently.

- Ransomware - how do countries across the development spectrum react? What are different parameters that may direct the reaction?
  - What makes the difference between a ransomware incident from a criminal dimension to an international security dimension
  - Skill, scope and speed
  - Impact (direct and trickle down risks)
  - Motivation (e.g. against a government or not)

    - Funding / financing of if the incident/attack
    - Right not to define the international peace and security threshold (remain a prerogative of states).

- The impact of cyber incidents on communities, individuals, or groups and the response of governments, are two dimensions in the conversation.

- Useful to consider the role played by supreme national audit institutions. Can they influence the government's reaction? What standards do they use or refer to come to meaningful and implementable recommendations, e.g. in the case of a cybersecurity incident? Is there at the international level agreement among supreme audit institutions on how to assess and evaluate the impact or cyber incidents.

- The Impacts of cyber incidents go much further than the systems being down. Human beings are also being impacted. It is encouraging that the human impact of incidents is gaining more attention.

- Countries, and in particular small countries are forced to join efforts to a cope with cyber incidents.

- At the national level, it is important to bring stakeholders together to share information, build trust and confidence between stakeholders, for capacity building, to identify strategies and actions to be taken in case of incidents, and to share an understanding of the emerging issues in the country and region.

- Collaboration between nations in the case of a cyber incident is important, but one should be aware that not all have the same capacity and expertise. Strategic collaboration and coordination within regions fosters the capability to address incidents. Trust and shared values facilitate the cooperation between the countries in a region.

- Citizen cyber hygiene becomes an important element in avoiding and addressing incidents and social engineering as more and more people use mobile banking and payment apps. The key messaging must be simple and shared across different channels to reach all parts of the population.

- Civil society can play an important role in (citizen) capacity building - and close cooperation between civil society and CIRTS is instrumental to share awareness of current and new threats and the measures and interventions that can be taken.

The audience raised the following questions during the Q&A session:

- How can international law be effectively applicable in case of cyber incidents?
- What are legal actions that can be taken by developing nations to hold cyber criminals accountable and claim compensation ?
- How to convince countries to disclose and share forensic evidence they collect?
- How effective and enforceable can political declarations on the non payment of ransomware be?
- How to establish cybersecurity policies that fit the perspective and logic of global south stakeholders when a large part depends on security permits, bodies from regions and organisations in the global north?
- Importance to include Members of Parliament in cyber discussions and capacity building
- What strategies are in place to prevent and fight cyber terrorims?
- Best practices at the citizen level are key but still too often lacking. How to avoid oversharing of data collection? Importance of visual penalties as a sign for citizens.
- How to share resources among stakeholders to avoid duplication and use resources efforts more effectively ?