Australia to Consider Banning Ransom Payments

Following recent cyber-attacks affecting millions of Australians, Australia's Home Affairs Minister Clare O'Neil stated that the Australian government would consider **making it illegal** to pay ransoms. When asked if the Australian government planned to look at outlawing ransom payments to cybercriminals, O'Neil stated "that's correct". The comments come after Australia formalized a new cyberpolicing model between the country's Federal Police and Australian Signals Directorate, which intercepts electronic communications from foreign countries to do 'new tough policing' on cybercrime. The new model will consist of 100 officers between each of the agencies which would act as a joint standing operation against cyber criminals.

Ransomware and BCDR Plans

In the event of a ransomware attack that impacts critical systems and sensitive information, you should have clear definitions of how your **Business Continuity and Disaster Recovery (BCDR)** plans relate to your ransomware response plans. Having a unique BCDR plan for ransomware is not necessarily needed, but existing BCDR plans should reference cybersecurity response if an event occurs. That cybersecurity response should refer to any disaster recovery processes when operations are affected, and the activities for resuming business operations after an event.

Advanced planning and exercising are essential, especially if multiple plans and teams are involved during a ransomware event. For example, a common challenge is the role of the IT team after the initial incident response by the cybersecurity team, and what role the BCDR team plays. The IT team may be participating at all stages by assessing the impact to technology and business operations, and they may be a key piece to understanding when to activate BCDR plans. Understanding the roles and responsibilities of each team and when to hand-off activities will ensure there is no confusion or processes overlooked.

How Denmark Became One of the Most Cyber-Secure Countries

After e-mail accounts for members of the Danish Defense were hacked in 2017, Denmark has taken measures to invest in and enhance their cybersecurity strategy to be rated the **world's most cyber-safe nation from 2019 – 2021**. This ranking was developed by Comparitech by using a list of 15 criteria focusing on percentages of users and devices targeted or impacted by malware, ransomware, IOT, and other security events.

Denmark has taken various initiatives to protect their citizens, including

- Use of multi-factor authentication across government and financial services
- Major investments in cyber and information security
- Cyber policy based on technological resilience, enhancing citizen knowledge and awareness, and improving coordination among actors
- Strong and well-developed banking apps
- Creating a **24/7 situation center** to build a national cyber situation picture
- **Launching an app** to provide information on digital scams, malware attacks, live updates from law enforcement and banks, and advise if a breach has occurred

Going forward, Denmark has adopted a **National Strategy for Cyber and Information Security** for 2022 – 2024 to include strategic objectives of protecting vital societal functions, improving skills and management in cybersecurity, strengthening public-private partnerships, and actively participating in global initiatives to fight cybercrime.

Hackers Exploit VPN Software Vulnerability

Cisco system has warned of an active exploitation attempt targeting several **security flaws** in their Cisco AnyConnect Secure Mobility Client for Windows. The vulnerabilities (**CVE-2020-3153** and **CVE-2020-3433**) could enable local authentication attackers to perform DLL hijacking and copy files to system directories with elevated privileges. A fix for CVE-2020-3153 was released in February 2022 and another fix for CVE-2020-3433 was released in August 2020. The alert comes as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) moved to add the two flaws to its **Known Exploited Vulnerabilities** catalog because of ongoing evidence of active abuse.

Ransomware Poses Big Threats to UK Orgs

Ransomware attacks against hospitals, schools and other organizations has been the biggest **cyberthreat the country has faced** in 2022. While organizations witnessed an increase in various attacks, it was the country's critical infrastructure that bore the brunt of attacks including **over a dozen incidents** that required national-level coordination to mitigate malware from systems such as the national emergency helpline, and water supply company.

This monthly update is brought to you by the Financial Services Information Sharing and Analysis Center (FS-ISAC) in coordination with the Investment Industry Association of Canada (IIAC), the International Council of Securities Associations (ICSA), the Financial Services Institute (FSI), the Insured Retirement Institute (IRI), the Securities Industry and Financial Markets Association (SIFMA) and the SPARK Institute.

The information provided in this monthly newsletter highlights cybersecurity topics and emerging threats to the securities industry globally. It is intended to increase the cybersecurity awareness of an organization's end-users and to help them interact in a more secure manner. This newsletter is not intended to replace the benefits of joining FS-ISAC. Learn more at fsisac.com.