Zyber Global

JULY 2024 | ISSUE 48

# MAKING DIGITAL SAFE WITH EXPERT CYBER SECURITY TRAINING

*Welcome to the July edition of Zyber Global Newsletter, the 48th edition! Uncover Key Cybersecurity Trends and Breakthroughs this July!*

*We've had a heatwave this week in London, and it's been a perfect time to enjoy the parks and outdoor activities. It has brought out the best of summer, with everyone soaking up the sun!*

*I attended the CyberFlex webinar and was thoroughly impressed with its comprehensive and interactive approach to online safety for young adults. CyberFlex combines actionable information with engaging tools, making it an essential resource for equipping 18 to 25-year-olds with the necessary skills to navigate the digital world safely.*

*This collaboration between the Global Cyber Alliance and Amazon has produced a well-rounded solution that not only educates but also empowers young adults to protect themselves against cyber threats. This initiative is a significant step towards creating a safer online environment for our youth.*

*I recently shared information about the CyberFlex launch widely with my network before this month's webinars. I hope many of you were able to join one of the sessions to learn about this fantastic new resource. If you missed it, you can still access the information and tools on their website at this link: CyberFlex Website.*

Esther George, CEO Zyber Global Centre

BEST REGARDS
ESTHER GEORGE

## This Month's Features

### Zyber Focus Article

PART 2- Crisis management: Damage control during cybersecurity incidents in large business systems by Damir Delija, Senior Lecturer, Digital Forensics and Cybersecurity, TVZ.

### Zyber News

A roundup of the latest international cybercrime news.

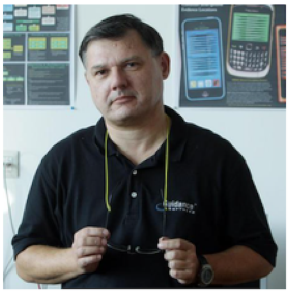
### Zyber Global Events Information

A focus on forums/conferences around the world.

*Remember to stay vigilant and informed, as we continue to navigate the ever-evolving landscape of cybersecurity.*

# Zyber Focus Article

## PART 2- Crisis management: Damage control during cybersecurity incidents in large business systems



**Damir Delija, Senior Lecturer, Digital Forensics and Cybersecurity, TVZ.**

In the previous newsletter, June 2024, 47th edition, Damir Delija explained that '*in a modern, digitally connected world, cybersecurity is key to protecting vital business operations. Effective management of cybersecurity incidents is essential not only to reduce immediate losses, but also to protect reputation and ensure the long-term sustainability of the enterprise. In order to control damage during cyber incidents, organizations need to focus on preparedness, rapid response and recovery strategies, taking into account complex contractual relationships and different legal regulations*'.
In this second and last part, he explores strategies for global recovery and business continuity.

**Strategies for global recovery and business continuity**
Once the immediate threat is addressed, the focus must be placed on global recovery and ensuring business continuity. This includes aligning the recovery with different legal requirements and operational standards in all countries where the organization operates. Analyzing and integrating the lessons learned from the incident are key to strengthening global resilience. As part of the recovery planning, it is necessary to work out proactive cooperation well and to carry out revisions of existing contracts, so as to avoid conflicts and vague relationships during the incident. Regular audits of contracts and legal obligations with partners can strengthen security protocols and ensure that all parties are adequately prepared for potential incidents. Working with legal and security professionals can help identify and minimize the risks arising from contractual relationships.

**Building a robust incident response plan**
The foundation of any well-prepared damage control strategy is a comprehensive incident response plan. This plan should include defining key roles and responsibilities, protocols for communication within the organization and with external parties, and detailed procedures for identifying, assessing, isolating and mitigating an incident. Comprehensive tests and regular simulations can help teams prepare for real situations. In the planning process, an important element is understanding that a plan however good it may be cannot cover all situations i.e. That it will be necessary to adapt the plan to the actual situation on the basis of monitoring how the procedures from the plan affect the development of the incident. Blindly following an existing plan can be more devastating than the impact of the incident itself. The process of planning, evaluation of plans, procedures and documentation should be carried out regularly, with the evaluation of changes in the organization, changes in threats and risks, as well as the introduction of possible new procedures and tools. One of the newest tools in the field is large-scale language models (LLMs), such as ChatGPT, which can significantly improve an organization's ability to respond quickly and efficiently to security incidents.

The use of LLM allows for a number of benefits, but also risks. Automating analysis and response, LLMs can analyze vast amounts of data — from logs to communication channels — to identify samples and potential causes of an incident. This ability allows organizations to quickly detect and respond to security threats, thereby reducing the time it takes to respond and reducing potential damage. Decision support, i.e. by integrating LLMs into security protocols, organizations can access recommendations based on data analysis to mitigate risk. These models can suggest steps for real-time remediation, ensuring that incident response teams have all the necessary information for informed decision-making.

Training and simulations, using LLMs, security teams can be trained through realistic simulations of cyberattacks. These models can generate scenarios based on the latest trends in cyber threats, enabling staff to practice and hone their skills in a safe, controlled environment.

During a security incident, it is crucial to maintain clear and consistent communication. LLMs can help formulate notifications for users and staff, explaining the nature of the incident and the recommended steps to take. This helps reduce panic and ensures that all interested parties adhere to the necessary protocols. LLMs can be integrated with existing incident management platforms to automate monitoring, reporting and incident responses. This integration enables the creation of a more efficient and coordinated response to incidents. Customer support plays a key role in managing user perceptions of security. LLMs can respond quickly to user inquiries, providing up-to-date information and advice on protecting personal and professional information. Through the application of these technologies, organizations can not only respond faster to incidents, but also work proactively to strengthen their security protocols, thereby increasing their overall resilience to cyber threats. LLM's powerful tool in, it is important to monitor their use with caution. Incorrect information or misinterpretations of data can lead to wrong decisions, therefore it is essential that their outputs are checked and validated through expert human supervision. The development of such an environment must be part of a strategic plan.

**Read more:**
**https://zyberglobal.com/blog**

# Zyber News Roundup

### U.S. record labels are suing AI music generators, alleging copyright infringement

Major record labels, including Universal, Sony, and Warner, have filed lawsuits against AI music companies Suno and Udio-maker Uncharted Labs. The labels allege that these companies used their copyrighted music to train AI models without permission, leading to realistic song generation that infringes on intellectual property.

The lawsuits, coordinated by the Recording Industry Association of America, seek to halt these practices and claim damages. Suno and Udio have been accused of evading transparency regarding their data sources, intensifying concerns about AI's impact on the music industry.

The music labels argue that such unlicensed use of AI tools sets back genuine innovation and undermines artists' rights and compensation. Despite the defendants' claims of ensuring no reproduction of copyrighted works, the lawsuits highlight the need for clearer regulations and ethical standards in the development and deployment of generative AI technologies in the music sector.

**Read more:**
https://www.nbcnews.com/tech/tech-news/us-record-labels-are-suing-ai-music-generators-alleging-copyright-infr-rcna158660#

### Ransomware victims are becoming less likely to pay up

Despite a significant increase in ransomware demands, fewer companies are paying up as they bolster their defenses against cyberattacks. Marsh's report shows that only 23% of 1,800 companies paid ransom demands in the past year, compared to 63% in 2021, highlighting improved resilience and higher ransom demands dissuading payments. The median ransom demand jumped to $20 million, but with enhanced security measures and the complex legal landscape involving sanctioned countries like Russia, businesses are increasingly prepared to handle attacks without succumbing to extortion.

This shift is also driven by the growing sophistication of executives in legal, risk, technology, and privacy areas, who have developed more robust strategies to mitigate the impact of ransomware attacks. Moreover, enhanced resiliency measures mean that even when companies are targeted, their operations are not fully impaired, reducing the necessity to pay ransoms. This trend, coupled with law enforcement's improved efforts to combat cybercriminals, signals a turning tide in the fight against ransomware.

**Read more:**
https://www.cybersecuritydive.com/news/ransomware-victims-becoming-less-likely-to-pay-cyberhackers-report/719470/

### UN body reviews allegations of Russian satellite interference

The International Telecommunications Union (ITU) is investigating complaints from Ukraine and several European countries about satellite interference affecting navigation services and television broadcasts. The interference, allegedly caused by Russia, has jammed GPS signals, potentially endangering air traffic control, and disrupted TV channels, including children's programs with violent war images.

Ukraine reported 11 instances of interference over the last three months, while France, Sweden, the Netherlands, and Luxembourg also reported similar issues. Russia denied the allegations, claiming compliance with ITU rules and accusing NATO countries of similar interference. The ITU's meeting aims to address and resolve these issues.

**Read more:**
https://www.reuters.com/world/un-body-reviews-allegations-russian-satellite-interference-2024-06-25/

### Manufacturing cybersecurity at heart of new White House guidance

The Department of Energy has released a new framework outlining best practices for securing clean energy cyber supply chains, highlighting the increased threat of cyberattacks on energy systems.

The Biden administration emphasized the urgency of these measures, noting the growing cyber threats to the energy sector from both foreign and domestic actors. In response to these threats, the administration established the White House Council on Supply Chain Resilience and allocated $30 million for research and development to improve the cybersecurity of clean energy resources. The DOE's guidelines aim to fortify U.S. manufacturing and supply chain security by promoting best practices and encouraging collaboration between suppliers and end users.

**Read more:**
https://www.cybersecuritydive.com/news/energy-department-cybersecurity-manufacturing-supply-chain-best-practices/719612/

# Zyber Global Events Information Page

## GLOBAL CYBERSECURITY EVENTS

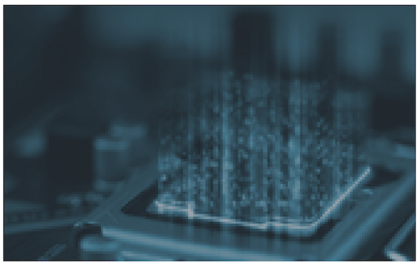
| 2024 APAC Summit<br>Singapore<br>9 - 10 July 2024 | Cybersecurity Summit<br>North Carolina, USA<br>16 July 2024 | Cyber Security EXPO<br>Manchester 2024<br>Manchester, UK<br>24 July 2024 |
|---|---|---|
| Join us at the Asia Pacific Summit 2024, an unmissable event that delves into the transformative trends reshaping the financial sector, including cloud, fintech, and cryptocurrencies.<br>Discover innovative approaches to reimagine cyber resiliency and effectively address complex and ever-evolving cyber risks in this new era. Stay ahead of the curve, navigate the dynamic cybersecurity landscape in the Asia Pacific region, and acquire valuable knowledge to stay informed on the latest developments.<br>Don't miss this opportunity to enhance your understanding and strategic preparedness in the evolving cybersecurity landscape. | Join us at the prestigious Second Annual Raleigh Cyber Security Summit.<br>Network with C-Suite and Senior Executives focused on protecting critical infrastructures, along with renowned information security experts and top solution providers.<br>Gain valuable insights from global experts on defending against cyber attacks. Engage in interactive panels and fast-track discussions to enhance knowledge and safeguard your organization. | The Cyber Security EXPO is a unique recruitment event!<br>It is exclusively tailored for clients and recruitment agencies in the cyber security industry.<br>Engage and network with numerous employers hiring for contract and permanent cyber roles.<br>Connect with hiring managers and recruitment agencies, uncovering hidden job opportunities.<br>Explore exhibiting companies and have one-on-one conversations with recruiters.<br>Attend speaker sessions to gain insights directly from employers in your sector. |
| **For further information**<br>**https://www.fsisac.com/events/2024-apac** | **For further information**<br>**https://cybersecuritysummit.com/summit/raleigh24/** | **For further information**<br>**https://www.cybersecurityexpo.co.uk/manchester** |

# Zyber Global Online Events

Our Online Courses with INsig2
Sign up now at https://insig2-and-zyberglobal.learnworlds.com/
Special discount: 15% Use Code: zyber

## Courses per sectors

**Legal Entities**
Customized courses for legal entities: judges, lawyers and public prosecutors.
Explore deeper aspects of digital forensics and the forensic value of evidence while collecting, processing, and presenting digital evidence in criminal and administrative proceedings.



**Law Enforcement**
Customized courses for law enforcement officials: First responders, forensic investigators and analysts.
Delve into procedures, techniques, and tools used in digital forensic analysis and how to apply them in forensic investigations.

**Private Sector Corporations and Small Businesses.**
Customized courses for industry professionals working in the private sector; to help them understand the value and the need for digital forensic, and its implications in a corporate environment.

## Course Structure

***FULL-TEXT REVISION**

***QUIZ AFTER EACH CHAPTER**

***CASE-STUDY AFTER FINAL EXAM**

c

At the end of each course, you will be issued a completion e-certificate which is immediately printable for your records. The number of **CPD** (Continuing Professional Development), **CPE** (Continuing Professional Education), and/or **CLE** (Continuing Legal Education) points will depend on the course.

### DISCOUNTS

Special discount for groups of 10+ participants on all courses. The bigger the group, the bigger the discount.

### BUNDLES

Stay on your forensic digital learning path and get the most from your e-learning experience by using course bundles.
https://bit.ly/31NRYsj

### FREE COURSE ON PASSWORD MANAGEMENT

This covers different lock security methods, guidelines on securely storing your passwords, various password managers and how to use them.
https://bit.ly/3eMu7ED