CS 7349
Data and Network Security
Case Study

Name: Bingying Liang
ID: 48999397

Due: Feb 19 2024

1. What are the main differences AND similarities between the above two reports? Note that the two companies are in different domains, but both are in the business of Enterprise Security. Please outline your responses CLEARLY, in your own words, in a MINIMUM of 1 page, with a MINIMUM of 5 differences and 3 similarities. This will help you compare and contrast multiple cybersecurity reports. Your responses need to be in the technical and business domains. E.g. "a difference between the two reports is one report is from 2022-2023, and the other report from 2023" OR "Radware report is 37 pages, while the Verizon DBIR is 89 pages", or similar responses on the format, appearance, length and design of the report will incur zero (0) marks. Cutting and pasting from the report, or other sources will result in a grade of zero.

   Solution:
   Differences:

   (a) Data Collection and Scope:

   - **Verizon DBIR:** Utilizes data contributed by global partners, including law enforcement and security firms, focusing on security incidents and confirmed data breaches across various industries. The report is grounded in the analysis of 16,312 security incidents, of which 5,199 were confirmed data breaches[1].
   - **Radware:** Gathers data from Radware devices deployed in cloud scrubbing centers and on-premise managed devices, alongside Radware's Global Deception Network (GDN). The emphasis is on DDoS events, volumes, web application attacks, and unsolicited network scanning and attack activity[2].

   (b) Analytical Focus and Methodology:

   - **Verizon DBIR:** Emphasizes the analysis of data breaches, using its own VERIS Framework for classification, and includes a detailed examination of the incidents' context, such as vectors, actors, and industries affected.

- **Radware:** Concentrates on DDoS attacks, web application security, and network scanning activities, analyzing trends and techniques in cyberattacks and their evolution over time.

(c) Report Length and Detail:

- **Verizon DBIR:** The Verizon DBIR provides a more extensive narrative, including a broad spectrum of data breaches and detailed statistical analysis, reflecting a comprehensive approach to understanding cybersecurity incidents.
- **Radware:** Radware's report, while also detailed, focuses more narrowly on technical specifics of attacks, including DDoS and web application vulnerabilities, and offers targeted insights into attack methodologies and trends.

(d) Target Audience and Utility:

- **Verizon DBIR:** Aims at a broad audience including cybersecurity professionals, policy makers, and business leaders, providing insights that can inform strategic security decisions.
- **Radware:** While also targeting cybersecurity professionals, it might appeal more to technical operational teams focused on defense mechanisms against specific types of cyberattacks like DDoS and web application threats.

(e) Temporal and Geographic Coverage:

- **Verizon DBIR:** Offers a yearly snapshot with a global perspective on data breaches, providing insights into regional variations and sector-specific trends.
- **Radware:** Provides an annual analysis as well, but with a focus that might be more skewed towards the technological aspects of global threats, particularly those impacting network and application security.

Similarities

(a) Purpose and Goal: Both reports aim to enhance cybersecurity resilience by providing data-driven insights into the threat landscape, helping organizations to better prepare and protect against cyber threats.

(b) Data-Driven Insights: Each report leverages extensive data collection and analysis to offer evidence-based findings on the nature and impact of cyber threats.

(c) Trend Analysis and Predictions: Verizon and Radware both identify current trends in cybersecurity threats and offer predictions for future developments, serving as valuable resources for planning and threat mitigation.

2. In the reports, please identify 5 emerging Application Security trends for 2023. What was the business impact, and projected business impact of these trends? (business impact can include loss in $; loss in reputation; restructuring and new investments; executive departures, brand and reputation loss). A MINIMUM of 1 page is expected. This will help you look for business impact in general if you were a CIO or CSO, putting forth policies to mitigate loss. (Hint: External lookup may be necessary; take an example from each emerging trend and search for impact. A small paragraph per emerging trend+impact).

Solution: Emerging Application Security Trends for 2023: After reviewing the detailed sections on web application attack activity from the Radware 2022 Global Threat Analysis Report and relevant sections from the 2023 Verizon Data Breach Investigations Report (DBIR), I've identified several emerging application security trends for 2023, their business impacts, and projected implications. These insights are crucial for CIOs and CSOs formulating policies to mitigate losses.

(a) Increase in Web Application and API Attacks The Radware report highlights a significant increase in web application transactions blocked due to security violations, with a notable 128% growth from 2021 to 2022. This trend indicates an exponential rise in attacks targeting web applications and APIs[2].

Business Impact: Companies face direct financial losses due to service disruptions and costs associated with incident response and mitigation. Indirect impacts include loss of customer trust, potential fines for data breaches, and long-term brand damage. For instance, the 2017 Equifax breach cost the company over $4 billion in total[7], illustrating the severe financial implications of web application vulnerabilities.

(b) Predictable Resource Location Attacks

These attacks, which exploit the predictable nature of resource locations in web applications, accounted for almost half of all attacks witnessed in 2022[2].

Business Impact: Such vulnerabilities can lead to unauthorized access to sensitive data, resulting in significant financial losses, regulatory fines, and mandatory investments in security enhancements and compliance measures. The Capital One breach in 2019, involving a similar vulnerability, led to a $80 million fine and substantial reputational damage.

(c) Code and SQL Injection Attacks

Code and SQL injection attacks remain prevalent[8], representing more than a quarter of all web application attacks, further exacerbated by the widespread Log4Shell exploit[2].

Business Impact: These attacks can lead to data breaches, system takeovers, and extensive financial liabilities. The 2019 incident involving British Airways, which was fined £183 million for a data breach resulting from an injection attack, underscores the financial and reputational risks.

(d) Retail & Wholesale Trade Industry Targeted

The retail and wholesale trade industry emerged as the most attacked sector, accounting for 25.3% of blocked web application attacks[2].

Business Impact: Attacks on this sector often aim at payment card data, leading to direct financial loss, customer compensation costs, increased cybersecurity spending, and sometimes executive reshuffles due to breach accountability. The Target breach in 2013, resulting in $162 million in expenses, highlights the severe implications for the retail sector.

(e) Use of Stolen Credentials and Ransomware in Professional Services

The Verizon DBIR indicates that ransomware and the use of stolen credentials are leading actions causing breaches in the professional services sector, emphasizing the

threat from credential theft and ransomware attacks[2].

Business Impact: Incidents involving ransomware or credential theft can halt business operations, necessitate ransom payments, and lead to significant recovery costs. The 2020 incident with Cognizant, a professional services company, involved a ransomware attack that led to an estimated $50-$70 million in losses, highlighting the impact of such threats.

These trends underline the evolving threat landscape facing web applications and the critical sectors of retail, wholesale trade, and professional services. For CIOs and CSOs, the business impacts of these trends underscore the necessity for robust security policies, proactive threat mitigation strategies, and continuous investment in cybersecurity defenses to protect against financial losses, reputational damage, and compliance penalties.

3. From the Verizon DBIR report, please summarize five (5) incidents, of different types, and their impact (e.g Do not give 2 DDoS incidents or 2 Supply Chain attack incidents. Provide 1 of each). These are specific attacks and their business impact.

   (a) what was the incident

   (b) how did the incident occur? (what vulnerability was exploited)

   (c) how was the vulnerability fixed (if at all, or if a fix was in place and not put in)

   (d) what was the impact? ($ loss, reputation, restructuring, etc).

   A MINIMUM of 1 page is expected. This will bring you up to speed on the top cybersecurity incidents of 2022. Your response must be clearly laid out (Hint: Use a table; do not restrict yourself to the reports. Responses should be numbered, with a) thru d) responses for each. Avoid single line responses).

   Solution: Below is a summary of five distinct cyber incidents from 2022, each demonstrating a different attack vector, their impacts, and, where applicable, the measures taken to address them. These examples underscore the multifaceted nature of cyber threats and their significant repercussions on businesses, governments, and individuals.

   (a) SuperVPN, GeckoVPN, and ChatVPN Data Breach
      - Incident: Personal information of 21 million users was leaked due to a breach in several Android VPN services.
      - How it Occurred: The breach exposed full names, usernames, country names, billing details, email addresses, and password strings[6].
      - Vulnerability Fix: Not specified.
      - Impact: Exposed sensitive user information, risking identity theft and privacy violations[4].

   (b) Costa Rica Government Ransomware Attack
      - Incident: The Conti ransomware gang attacked the Costa Rican government[6], stealing and leaking 670GB of data.

- How it Occurred: Through ransomware deployment, exploiting system vulnerabilities.
- Vulnerability Fix: Response included declaring a state of emergency; specific mitigation steps not detailed.
- Impact: Significant data compromise and a demanded ransom of $20 million [4].

(c) LAUSD Data Breach by Vice Society

- The Los Angeles Unified School District suffered a breach, leading to the leak of 500GB of sensitive information.
- How it Occurred: The district did not meet the ransom demands of the Russian-speaking hacking group Vice Society.
- Vulnerability Fix: Not specified, though the incident highlights the need for improved cybersecurity measures in the education sector.
- Impact: Exposed personal identifying information, posing risks to privacy and security of staff and students[4].

(d) Iranian Phishing Campaign Against Jordan Ministry of Foreign Affairs

- Incident: A phishing campaign targeted Jordan's Ministry of Foreign Affairs, attributed to Iranian cyber espionage actors.
- How it Occurred: Via email phishing, attempting to compromise official communications.
- Vulnerability Fix: The attack's success and the specifics of any countermeasures were not disclosed.
- Impact: Potential access to sensitive diplomatic communications and data[5].

(e) DDoS Attack on Lithuania's Infrastructure

- Incident: Lithuanian state railway, airports, media companies, and government ministries faced DDoS attacks.
- How it Occurred: A Russian-backed hacking group executed the attacks, overwhelming the targets' online services.
- Vulnerability Fix: Details on the resolution are not provided, but such incidents often lead to strengthening of network defenses.
- Impact: Disrupted government operations and public services, highlighting vulnerabilities in national infrastructure[5].

These incidents illustrate the varied tactics cybercriminals use, including ransomware, data breaches, phishing, and DDoS attacks, to exploit vulnerabilities across different sectors. They underscore the critical importance of robust cybersecurity measures, ongoing vigilance, and the potential need for legislative responses to combat ransomware and other cyber threats. The impacts range from significant financial demands, exposure of sensitive personal and governmental information, to disruptions in critical public services, emphasizing the need for comprehensive cybersecurity strategies to protect against such diverse and evolving threats

4. What do the reports outline as next steps (mitigation approaches) for 2023. 3 approaches from Radware and 3 approaches from Verizon are requested. The goal is to compare the focus from 2 different companies, in different domains, looking at the same problem of how to secure IT in enterprises. A MINIMUM of 1 page is expected. Feel free to use other references.

   Solution: To address the request for outlining mitigation approaches for 2023 from the Radware 2022 Global Threat Analysis Report and the 2023 Verizon Data Breach Investigations Report (DBIR), I've synthesized the available insights from the Verizon DBIR and integrated external research to supplement the missing direct mitigation strategies from the Radware report.

   Verizon's Mitigation Approaches for 2023:

   (a) Secure Configuration and Network Management:
   Establishing and maintaining a secure configuration process for enterprise assets and software, including implementing and managing firewalls on servers and end-user devices, is crucial. This approach aims to reduce the attack surface and protect against unauthorized access[1].

   (b) Email and Web Browser Protection:
   Utilizing DNS filtering services to protect against malicious websites and phishing attacks. This is a proactive measure to prevent malware infections and data breaches originating from email and web browsing activities[1].

   (c) Continuous Vulnerability Management:
   A structured vulnerability management process, paired with a consistent remediation process, helps in promptly addressing known security weaknesses. Automated backups and secure data recovery processes are emphasized to ensure business continuity in the event of a breach[1].

   Radware's Mitigation Approaches for 2023 (Inferred from General Best Practices in Cybersecurity):

   (a) Enhanced DDoS Protection:
   Given Radware's focus on DDoS events, enhancing DDoS protection measures is a logical step. This includes deploying advanced DDoS mitigation tools and services that can dynamically adapt to evolving attack vectors, ensuring availability and continuity of services.

   (b) Application Security:
   Strengthening web application firewalls (WAFs) and implementing rigorous application security testing can mitigate web application attacks. This involves regular security assessments, code reviews, and deploying automated solutions to detect and block attacks in real-time.

   (c) Threat Intelligence and Behavioral Analysis: Utilizing Radware's Global Deception Network (GDN) insights for threat intelligence, focusing on understanding attack patterns, and applying behavioral analysis to detect anomalies. This proactive stance allows for the early detection of potential threats and swift response to mitigate risks.

Comparative Analysis:

- Verizon DBIR emphasizes foundational cybersecurity practices, focusing on securing configurations, protecting against common threat vectors like email and web-based threats, and maintaining a strong posture against vulnerabilities. The DBIR's approach is comprehensive, covering a wide range of cybersecurity fundamentals that apply across various sectors and organization sizes.
- Radware's Approach (inferred from general best practices and their focus areas), suggests a technical and specific focus on mitigating DDoS and web application attacks, leveraging advanced detection mechanisms and threat intelligence. Radware's strategies are likely to emphasize leveraging technology and intelligence to combat sophisticated and evolving threats.

While both Verizon and Radware aim at enhancing cybersecurity resilience, their approaches reflect their operational focus areas—Verizon with a broad, foundational approach, and Radware with a more targeted, technically sophisticated stance against specific types of cyber threats. This comparison underscores the diverse strategies that organizations may need to employ, combining foundational cybersecurity practices with advanced, targeted defenses to comprehensively protect against the evolving threat landscape.

5. What are the overall trends expected globally in 2024? Using the WEF Report, please identify 2024

   (a) 5 major trends

   (b) give 2 examples for each trend.

   A MINIMUM of 2 pages is expected. Use external references wherever necessary to support your responses.

   Solution:
   Analyzing the World Economic Forum's Global Cybersecurity Outlook for 2024 reveals significant insights into the cybersecurity landscape and its expected developments. The report outlines several critical trends that will shape the global cybersecurity domain in the upcoming year, focusing on the challenges and strategic responses necessary for organizations. Here, we delve into five major trends for 2024, providing two examples for each to illustrate their implications and potential impacts.

   (a) Growing Cyber Inequity

   The disparity between organizations capable of maintaining cyber resilience and those struggling continues to grow, especially affecting small and medium enterprises (SMEs). This widening gap is driven by advances in adversarial capabilities, such as phishing, malware, and deepfakes, exacerbated by the rapid development and adoption of emerging technologies like generative AI.

   Examples:

- SME Vulnerabilities: SMEs are particularly vulnerable, with many lacking the necessary cyber resilience to meet critical operational requirements. This vulnerability is highlighted by the statistic that half of the smallest organizations by revenue are unsure if they have the skills needed to meet their cyber objectives..
- The digital transformation accelerated by the COVID-19 pandemic has seen many businesses increase their online presence. However, without adequate cybersecurity measures, these businesses expose themselves to increased risk, further widening the gap between cyber-resilient and vulnerable organizations[3].

(b) Skills and Talent Shortage There is a huge disparity in skills and talent in cybersecurity. Many small organizations don't have or aren't sure if they have the necessary skills to achieve their cybersecurity goals. This shortage is a key challenge in designing a resilient cybersecurity infrastructure.

Examples:

- Skills gap in small organizations: Small organizations are more likely to report a lack of necessary skills, and many organizations say they don't have the skills they need to achieve their network goals.
- Cybersecurity education and training programs are struggling to keep pace with the rapidly evolving threat landscape, leading to a scenario where even organizations willing to invest in cybersecurity cannot find adequately trained personnel[3].

(c) Cyber-Business Alignment

There is an increasing alignment between cybersecurity and business objectives, with organizations recognizing the importance of integrating cybersecurity into strategic business planning. This trend is critical for fostering a secure, resilient, and trustworthy digital future.

Examples:

- Increased CEO Engagement: A significant number of organizations now report a direct link between their cyber resilience and CEO engagement, with those considered cyber-resilient much more likely to trust their CEO to speak externally about cyber risks.
- Legacy Technology and Processes: The challenge of transforming legacy technology and processes is cited as a major barrier to achieving cyber resilience, indicating a focus on updating and securing outdated systems.
- The rise in material cyber incidents affecting businesses highlights the need for executive leadership to understand and act on cybersecurity intelligence, integrating it into strategic planning and risk management processes[3].

(d) Cyber Ecosystem Risks

The risks associated with cybersecurity are extending beyond individual organizations to encompass entire ecosystems. Partners within an ecosystem can both significantly support and hinder efforts to achieve cybersecurity goals.

Examples:

- Third-Party Incidents: A significant portion of organizations attribute material cyber incidents to third parties, underscoring the importance of managing supply

chain and partner risks.

- Supply Chain Vulnerabilities: Many organizations admit to having an insufficient understanding of their supply chain vulnerabilities, highlighting the need for better visibility and management of third-party risks.
- Third-party vendor risks are increasingly becoming a focal point for cybersecurity strategies, as seen in the numerous breaches originating from compromised suppliers or service providers. Organizations are now more diligently assessing the cybersecurity posture of their partners[3].

(e) Regulatory Influence on Cybersecurity The role of cyber and privacy regulations in mitigating risks is increasingly recognized, with a growing number of executives believing in their effectiveness. This trend underscores the importance of compliance and the role of legislation in shaping cybersecurity practices.

Examples:

- Positive View on Regulations: A notable increase in executives who view cyber and privacy regulations as effective in reducing risks within their organization's ecosystem.
- Third-Party Risk Visibility: Despite the challenges, there is an acknowledgment of the need for better visibility of third-party risks, with efforts to improve understanding and management of these vulnerabilities.
- The role of cyber insurance is evolving from a mere financial risk transfer mechanism to an integral part of cybersecurity strategy, encouraging better risk management practices and facilitating recovery from cyber incidents. This shift underscores the importance of a collaborative approach to cyber resilience, involving insurers in the broader cybersecurity ecosystem[2].

These trends highlight the complex and evolving nature of cybersecurity challenges facing organizations globally. Addressing these challenges requires a multi-faceted approach, including enhancing cyber resilience[9], bridging the skills gap, fostering alignment between cybersecurity and business objectives, managing ecosystem risks, and adhering to regulatory requirements.

References

[1] Verizon, "2023 Data Breach Investigations Report," *Verizon Communications*, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[2] Radware, "Radware 2022 Global Threat Analysis Report," *Radware Ltd*, 2022. [Online]. Available: https://www.radware.com/SecurityReport-2022/

[3] World Economic Forum, "Global Cybersecurity Outlook 2024," *World Economic Forum*, 2024. [Online]. Available: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdff

[4] Security Magazine, "The Top 10 Data Breaches of 2022," *BNP Media*, 2022. [Online]. Available: https://www.securitymagazine.com/articles/98716-the-top-10-data-breaches-of-2022.

[5] Center for Strategic and International Studies (CSIS), "Significant Cyber Incidents," *CSIS*, 2024. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[6] T. Ansari, 'The Biggest Data Breaches Of 2022', Analytics India Magazine. [Online]. Available: https://analyticsindiamag.com/the-biggest-data-breaches-of-2022/

[7] calexi, 'Cybersecurity Training Education', Tonex Training. [Online]. Available: https://www.tonex.com/cybersecurity-training-education/

[8] Comodo, 'Types of Network Attacks — Top 6 Network Security Attack Types 2023', Cwatch Web Security. [Online]. Available: https://cwatch.comodo.com/types-of-network-attacks.php

[9] 'https://www.dailyexcelsior.com/cybersecurity-challenges-in-india/?cv=1'. [Online]. Available: https://www.dailyexcelsior.com/cybersecurity-challenges-in-india/?cv=1