Threat ID Threat type Threat description Threat Event ID Threat Event description Likelihood Consequence Current threat level Cybersecurity protection measures Expected effectiveness (1-5) New threat level

T1 Credential stuffing Attackers exploit reused login credentials NA NA High Unauthorized access, data theft High Multi-factor authentication, account monitoring, password policies 4 Moderate

T2 Cloud vulnerabilities Inadequate security configurations in cloud services NA NA Moderate Data breaches, compliance violations High Regular security audits, encryption, access controls 3 Low

T3 Denial of Service (DoS) Flood network with excessive traffic, causing unavailability NA NA High Disrupted operations, financial loss High DDoS protection services, traffic filtering, server scalability 4 Moderate

T4 Fake news Spread misinformation through social media NA NA Common Manipulated public opinion High Media literacy education, fact-checking tools, content moderation 5 Moderate

T5 Formjacking Inject malicious code into online payment pages NA NA Moderate Stolen payment details High Secure payment gateways, website security audits, user education 4 Moderate

T6 Inadequate patch management Failure to update software and systems NA NA Moderate Increased risk of exploits Moderate Patch management policies, automated update systems, vulnerability scanning 3 Low

T7 Insider threat Malicious or negligent actions by insiders NA NA Moderate Data leaks, system sabotage Moderate Access controls, user monitoring, employee training 4 Moderate

T8 IoT vulnerabilities Insecure smart devices lacking proper security measures NA NA High Compromised privacy, network security High Firmware updates, network segmentation, device authentication 4 Moderate

T9 Malware Malicious software infecting computers and networks NA NA High Data theft, system disruption High Antivirus software, malware detection tools, user education 4 Moderate

T10 Man-in-the-middle attack Intercepting and altering communication between parties NA NA Moderate Eavesdropping, data manipulation High Encryption, secure communication protocols, network monitoring 4 Moderate

T11 Shadow IT systems Unauthorized use of software or services by employees NA NA Moderate Data breaches, compliance violations High Employee training, access controls, policy enforcement 4 Moderate

T12 Social engineering Manipulating individuals to disclose sensitive information NA NA High Data breaches, financial loss High Employee training, awareness campaigns, incident response plans 4 Moderate

T13 Synthetic identities Creation of fake identities for fraudulent purposes NA NA Moderate Identity theft, financial fraud High Identity verification processes, fraud detection algorithms, user education 4 Moderate

T14 Wi-Fi security vulnerabilities Insecure Wi-Fi networks and protocols NA NA High Eavesdropping, data interception High Strong encryption, secure Wi-Fi protocols, network segment

Threat ID Threat type Threat description Threat Event ID Threat Event description Likelihood Consequence Current threat level Cybersecurity protection measures Expected effectiveness (1-5) New threat level

T1 Adware Malicious software displaying pop-ups/ads to generate revenue via user clicks NA NA Moderate User irritation, potential data exposure Moderate Anti-adware software, ad-blocking extensions, user education 3 Low

T2 Bot (and botnets) Infected computer controlled remotely by hacker to launch attacks or join botnet NA NA High System compromise, data theft High Botnet detection tools, network monitoring, user education 4 Moderate

T3 Rootkit Hidden software allowing remote control of computer by cybercriminals NA NA High Unauthorized access, data theft High Rootkit detection software, regular system scans, firmware updates 4 Moderate

T4 Spam Unsolicited commercial or bulk email sent for monetary gain by interaction with recipients NA NA High Email overload, potential phishing High Spam filters, email authentication protocols, user training 4 Moderate

T5 Spyware Software secretly recording online activity to collect personal information NA NA High Privacy invasion, identity theft High Anti-spyware software, firewall protection, user education 4 Moderate

T6 Trojan horse Malicious program disguised as legitimate file, initiating attack when active NA NA High System compromise, data loss High Antivirus software, email/file scanning, user awareness 4 Moderate

T7 Virus Malicious program altering device operations and spreading to other devices NA NA High System corruption, data loss High Antivirus software, regular system scans, user education 4 Moderate

T8 Worm Self-replicating virus spreading across network, causing system slowdown NA NA High Network congestion, system disruption High Network segmentation, patch management, user awareness 4 Moderate