

Annex – Notable Cybersecurity Incidents in Critical Sectors Globally

Water Sector | Servicios de Agua y Drenaje de Monterrey (SADM) , Mexico

Attempted Intrusion (Apr 2026)

SADM, a municipal water and drainage utility in Mexico, was targeted by an unknown threat actor. The threat actor leveraged Anthropic's Claude and OpenAI's GPT AI models to carry out the core intrusion activities. While attempts to breach the operational technology (OT) environment were unsuccessful, this incident highlighted how AI models may be used to help threat actors to better identify OT environments and develop viable access pathways into OT infrastructure.

Healthcare Sector | ChipSoft, Netherlands

Ransomware attack (Apr 2026)

Healthcare software provider ChipSoft suffered a ransomware attack, prompting it to disconnect services including its patient portals, HiX Mobile applications and Zorgplatform data exchange platform. While core patient care services were able to continue, hospitals and healthcare providers faced disruptions to digital information exchange and other non-core patient-facing services. Forensic investigations subsequently confirmed that patient personal and medical records from some Dutch healthcare institutions were stolen.

Healthcare Sector | University of Mississippi Medical Centre (UMMC), United States

Ransomware attack (Feb 2026)

UMMC suffered a significant ransomware attack that forced the organisation to shut down most of its IT systems, including access to its Epic Electronic Health Records (EHR) system. The disruption affected UMMC's seven hospitals and 35 clinics. All 35 clinics closed, elective procedures and imaging appointments were cancelled, and healthcare staff had to rely on manual and paper-based processes to continue urgent care. Normal clinic operations resumed after nine days.

Infocomm Sector | Singapore telecommunications providers, Singapore

Sustained Campaign (Feb 2026)

All four of Singapore's major telecommunications operators were disclosed to have been the target of a deliberate and sustained campaign by an Advanced Persistent Threat (APT) actor. Using techniques including zero-day exploits and rootkits, the threat actor gained unauthorised access to parts of telco networks and exfiltrated limited technical data, although no service disruption or compromise of sensitive customer data was detected.

Infocomm Sector | SK Telecom, South Korea

Exfiltration of customer records (April 2025)

South Korea's largest mobile operator, SK Telecom, disclosed a major cyber incident involving the compromise of systems supporting its mobile network. Government investigators identified 28 infected servers and 33 malware strains, including the BPFDoor backdoor, and found that approximately 26.96 million IMSI records had been exposed. The threat actor had gained access to SK Telecom's system-management network and compromised its Home Subscriber Server infrastructure, from which sensitive USIM-related information was subsequently exfiltrated.

Banking & Finance Sector | Marquis Software Solutions, United States*Ransomware attack (Aug 2025)*

Marquis Software Solutions, a technology provider serving US banks and credit unions, suffered a ransomware attack that exposed personal and financial information of over 670,000 individuals. The compromised data included names, addresses, dates of birth, Social Security numbers or taxpayer-identification numbers, and financial-account information. The incident highlighted the potential cascading impact of compromises involving third-party service providers, where a breach of a single provider can expose data belonging to customers across multiple organisations without the organisations themselves being directly compromised.

Banking & Finance Sector | Bank Rakyat, Malaysia*Exfiltration of sensitive information (Sep 2024)*

Bank Rakyat reported a cyber incident involving unauthorised access to its IT infrastructure in September 2024, in which a threat actor claimed to have stolen over 460 gigabytes of data. The bank subsequently implemented measures to strengthen its technology infrastructure, cybersecurity controls and operational processes.

Security & Emergency Sector | CodeRED Emergency Notification Platform, United States*Service disruption (Nov 2025)*

The OnSolve CodeRED emergency notification platform suffered a cyber-attack, disrupting a service used by state and local governments, police, fire departments and emergency-management organisations across the United States to issue evacuation notices, severe-weather warnings and other public-safety alerts. The compromise was sufficiently serious that the affected legacy CodeRED system was subsequently decommissioned, requiring affected jurisdictions to rely on alternative notification channels.

Government Sector | Ukraine State Registries, Ukraine*Service disruption (Dec 2024)*

Ukraine suffered a major cyber-attack against infrastructure supporting its Ministry of Justice state registries, forcing the government to suspend systems used for civil status records, businesses, property ownership and other core administrative functions. The disruption also affected processes at border crossings and customs, demonstrating how dependencies on common digital government infrastructure can result in cascading disruptions across multiple public services.

Government Sector | Indonesia National Data Centre, Indonesia*Ransomware attack (Jun 2024)*

Indonesia's Temporary National Data Centre experienced a ransomware attack which disrupted digital services across government, including immigration systems at major airports. More than 200 public agencies were affected.

Media Sector | VGTRK, Russia*Service disruption (Oct 2024)*

Russia's national state television and radio broadcaster VGTRK suffered a major cyber-attack that affected its digital and internal infrastructure. Online services were disrupted, and reporting indicated interruptions to some television programming, although VGTRK stated that its main radio and television broadcasting operations continued.