ILLUSTRATIVE INCIDENT INTELLIGENCE REPORT · CANADA

WHEN THE NETWORK BECOMES THE VULNERABILITY

12 Illustrative Cybersecurity & Physical Security Incidents
in Canadian Residential Condominium Properties

12	8	5	$2.1M+
Incidents documented	Canadian cities	Vulnerability types	Est. combined loss

IMPORTANT NOTICE: All incidents described in this document are entirely fictional and created for illustrative purposes only. They are designed to demonstrate real-world consequences of the network and physical security vulnerabilities commonly identified during Mycondolink technology audits. Any resemblance to actual events, buildings, persons, or corporations is coincidental. No real building names, addresses, residents, or individuals are referenced. This document is intended exclusively for use in Board presentations and property manager education.

INCIDENT INDEX

INC-001

The Cloned Fob Ring

HIGH | THEFT | Toronto, ON · 2024 · 312-unit building

Incident type	Coordinated theft — targeted suite entries across multiple floors
Duration	Approximately 11 weeks before detection
Estimated loss	$187,000 in electronics, jewellery, and cash across 23 affected suites
How detected	Resident reported missing laptop; security footage showed unknown individual using fob
Vulnerability root	125kHz EM4100 fob technology — cloneable in under 10 seconds

INCIDENT NARRATIVE

In the spring of 2024, residents of a 312-unit highrise in Toronto's east end began reporting missing items — laptops, jewellery, cash, and small electronics. In each case, there was no sign of forced entry. Doors were undamaged. Nothing appeared broken. Management initially assumed residents were misplacing items or that the incidents were unrelated.

When a resident reviewed their personal doorbell camera footage and saw an unfamiliar man entering their unit with what appeared to be a fob, they reported it to management and requested a police investigation. The police reviewed the building's camera system — which had been operating on a single NVR recording to a shared drive — and found that 19 days of footage had been overwritten due to insufficient storage. The footage that remained showed the same individual entering five different suites across three floors on separate occasions.

Investigators worked with a security consultant to analyse the access control logs. The building was using 125kHz proximity fobs — a technology with no encryption, no rolling codes, and no challenge-response protocol. The consultant demonstrated that the individual had almost certainly used a commercially available RFID cloning device to copy fobs in the elevator or lobby — likely obtained during brief social contact with residents. The cloned fobs left no distinct record in the access log because they presented the same UID as the original. There was no way to distinguish the legitimate holder from the clone.

The building had no audit log review process and no alerts configured for after-hours access. Management was unaware that the access control system even had a logging function. The individual was never apprehended. The corporation faced insurance claims totalling $187,000 and a class action inquiry from affected residents.

VULNERABILITIES EXPLOITED

- 125kHz fob technology with no encryption — credential duplication took under 10 seconds
- No audit log review process — incidents spanned 11 weeks without a single alert
- NVR with insufficient storage — footage overwrote itself before investigation commenced
- No duplicate credential detection — cloned UIDs appeared identical to legitimate credentials
- No after-hours access alerts — repeated late-night entries went unnoticed by management

LESSON: Encrypted credential technology (MIFARE DESFire EV2 or SEOS) eliminates cloning attacks entirely. Audit log review — even a weekly 10-minute check of after-hours access events — would have flagged this within days. NVR storage must be sized for a minimum 30-day retention window.

INC-002 The Dark Web Drone Drop

HIGH | DRUG TRAFFICKING | Vancouver, BC · 2023 · 228-unit building

Incident type	Commercial drug distribution operation run from a residential unit
Duration	Approximately 7 months before police operation
Estimated scale	Police seized narcotics with estimated street value of $340,000
How detected	Tip to Vancouver Police; subsequently reviewed building network and camera data
Vulnerability root	Camera system on shared LAN — footage accessible and deletable from any connected device

INCIDENT NARRATIVE

Vancouver Police received a tip in late 2023 that a residential unit in a 228-unit building in the False Creek area was being used as a distribution hub for fentanyl and methamphetamine. The operation, which had reportedly been running for approximately seven months, was sophisticated: orders were placed through encrypted messaging apps, payments made in cryptocurrency, and deliveries arranged using a commercial drone to drop packages onto the unit's balcony from a nearby park — avoiding any need for foot traffic into the building.

When police executed a search warrant, they discovered that the occupant — a short-term rental tenant who had sublet the unit in violation of the building's rules — had also compromised the building's camera system. Because the NVR and all IP cameras were on the same flat network as the building's Wi-Fi, and the NVR was accessible using its factory-default username and password, the tenant had been able to access the camera management interface from their unit and periodically delete recordings covering their floor and the lobby during delivery windows.

Management had no idea the camera system could be accessed by anyone on the building network. The NVR had never been audited. The default credentials had been in place since the system was installed four years earlier. Police were unable to retrieve any camera footage from the 6-hour windows surrounding each delivery — there were 23 such gaps across the 7-month period. The corporation subsequently faced a civil claim from three residents who argued the building had failed in its duty of care by maintaining an inadequate and unsecured surveillance system.

VULNERABILITIES EXPLOITED

- NVR accessible from building LAN using factory-default credentials — never changed since installation
- No network segmentation — camera system shared flat LAN with all resident Wi-Fi and building systems
- No NVR access logging — deletions went undetected until police investigation
- No short-term rental monitoring or guest credential controls in access control system
- No firewall between residential network segments and building management systems

LESSON: Camera systems must be on an isolated VLAN with firewall rules permitting access only from the security desk and management office — never from resident or guest Wi-Fi. NVR credentials must be changed on installation and audited annually. Access logging on the NVR itself provides an audit trail if recordings are tampered with.

INC-003 The Invisible Stalker

CRITICAL | STALKING | Ottawa, ON · 2024 · 180-unit building

Incident type	Stalking and harassment campaign enabled by compromised building camera access
Duration	Approximately 4 months before source identified
Impact	Victim obtained emergency protection order; perpetrator charged under Criminal Code s.264
How detected	Victim noticed perpetrator appearing at locations they had not publicly disclosed
Vulnerability root	Camera system port-forwarded to internet; credentials known to former building staff member

INCIDENT NARRATIVE

A resident of a 180-unit mid-rise in Ottawa began noticing in early 2024 that a former partner — against whom they had an existing peace bond — seemed to know their schedule in remarkable detail. The individual would appear near the building's entrance, in the parking garage, or at nearby locations at times that corresponded precisely to the resident's movements in and out of the building.

After reporting their concerns to police, investigators subpoenaed the building's ISP records and discovered that the building's camera NVR had been configured with a port forward that made its web interface accessible from any internet-connected device. The system was using its original installer password — which had been known to the perpetrator, who had briefly worked as a casual maintenance contractor for the building two years prior and had never had their access credentials revoked or changed after their contract ended.

For four months, the perpetrator had been accessing the live camera feeds remotely from their home — watching the lobby, the elevator bank, and the underground parking entrance in real time — enabling them to track the victim's exact movements without ever physically entering the building. Because the NVR had no access logging enabled, there was no record of the remote sessions in the system itself. The only evidence came from ISP connection logs.

The building's board faced a complaint to the Ontario Privacy Commissioner and a civil claim from the resident, who argued that the building's failure to secure the camera system and revoke former contractor access had materially enabled the harassment. The complaint was upheld.

VULNERABILITIES EXPLOITED

- Camera NVR port-forwarded to public internet — live feeds accessible from any IP address globally
- Contractor credentials never revoked or changed after contract ended — two-year-old password still active
- No NVR access logging — remote viewing sessions left no record in the building system
- No annual credential audit — no process to identify and deactivate former staff/contractor system access
- No firewall monitoring — port forward rule had been in place since original installation, never reviewed

LESSON: Contractor and vendor system credentials must be revoked the day a contract ends — not eventually. A semi-annual credential audit covering all building systems (not just door fobs) would catch this. No camera system should ever be port-forwarded to the internet. VPN-based remote access with MFA is the only acceptable method for legitimate remote viewing.

INC-004

The Parking Garage Strippers

HIGH | THEFT | Calgary, AB · 2023 · 400-unit building

Incident type	Organised vehicle theft ring — catalytic converters and vehicle parts
Duration	Approximately 9 weeks, 3 nights per week
Estimated loss	$94,000 in vehicle damage and stolen parts across 41 vehicles
How detected	Resident discovered damage and reviewed personal dashcam footage
Vulnerability root	Parking garage camera system offline for 6 weeks due to NVR on failed UPS; REX sensor bypass on garage pedestrian door

INCIDENT NARRATIVE

Residents of a 400-unit tower in Calgary's Beltline neighbourhood began reporting vehicle damage in the underground parkade in late 2023. Catalytic converters were being removed with angle grinders, and some vehicles had entire wiring harnesses stripped. Management reviewed the parking garage camera system and found it had been offline for six weeks — the NVR had lost power when the UPS it was connected to failed silently. No alert had been sent. No one had noticed. The recording gap was complete.

A forensic review of the building's access logs showed no anomalous fob entries during the incident windows. The thieves had not used the main vehicle entrance — they had used a pedestrian door on the north side of the garage that was secured with a proximity reader but whose request-to-exit sensor could be triggered from outside by inserting a thin tool through the door gap and activating the infrared sensor, releasing the latch without a credential. This bypass method — known in the industry — is trivial on doors without protective covers on the REX sensor.

The corporation's insurance claim was partially denied on the grounds that the camera system had been non-operational for an extended period without management knowledge, which the insurer characterised as a failure to maintain adequate security infrastructure. The insurer's position was that had the UPS failure triggered an alert, the outage could have been addressed within days and the extended period of unrecorded access would not have occurred.

VULNERABILITIES EXPLOITED

- Failed UPS on NVR — consumer-grade unit failed silently with no alert, system offline for 6 weeks
- No NVR health monitoring — camera recording failure undetected by management
- REX sensor bypass on parking pedestrian door — no protective cover, triggerable from outside through door gap
- No redundant recording or offsite storage — gap was total with no recovery possible
- No UPS battery test regime — failing unit had not been tested in over 3 years

LESSON: UPS units must be load-tested annually — a unit that appears functional can have zero effective runtime with a failed battery. NVR health monitoring should send an email or SMS alert within 15 minutes of any recording interruption. REX sensors in vehicle and pedestrian access doors require shrouded protective covers that prevent external manipulation.

INC-005

The Superintendent's Backdoor

CRITICAL | FRAUD | Mississauga, ON · 2024 · 156-unit building

Incident type	Insider fraud — former superintendent created persistent network backdoor
Duration	Remote access maintained for 14 months after employment termination
Estimated loss	$62,000 in fraudulent invoices submitted through compromised management system
How detected	New IT vendor discovered unknown TeamViewer session during routine maintenance
Vulnerability root	No off-boarding procedure for IT system credentials; no firewall; remote access unmonitored

INCIDENT NARRATIVE

A 156-unit lowrise in Mississauga dismissed its live-in superintendent in early 2023 following a performance dispute. Standard off-boarding was completed: the superintendent returned their master fob, vacated the unit, and their name was removed from the building directory. No one thought to review or revoke their access to the building's IT systems.

The superintendent had, during their tenure, installed TeamViewer on the management office PC — ostensibly for IT support purposes. The installation had never been documented, audited, or approved by the board. After termination, the individual retained the TeamViewer credentials and continued to access the management PC remotely. Because the building had no firewall, no network monitoring, and no endpoint security on the office workstation, the sessions were completely invisible to management.

Over the following 14 months, the former superintendent used the remote access to review the building's vendor contacts and invoice approval workflows. They then created fraudulent invoices under a shell company name and submitted them through a property management email address they had retained access to — the shared management@[building] account whose password had never been changed. A total of $62,000 in fraudulent invoices for 'maintenance services' were approved and paid before a new property manager flagged a duplicate vendor name and initiated an audit.

Police charged the individual with fraud over $5,000 and unauthorised use of a computer. The corporation recovered approximately $28,000 through insurance. The remaining $34,000 was written off. The board subsequently commissioned a full IT audit of all systems — the first in the building's 12-year history.

VULNERABILITIES EXPLOITED

- No IT credential off-boarding — remote access tools and email accounts not revoked on termination
- Undocumented TeamViewer installation — no inventory of remote access tools on building systems
- Shared email account with unchanged password — accessible by former employee indefinitely
- No network monitoring or firewall — remote sessions undetectable
- No remote access MFA — TeamViewer session required only the static password set at installation

LESSON: IT off-boarding must be a documented checklist item alongside physical key/fob return. Every remote access tool on every building system must be inventoried. Shared system accounts must have passwords changed whenever a staff member with access departs. MFA on all remote access tools eliminates this class of attack entirely.

INC-006

The Camera Blackout Burglaries

HIGH | BREAK & ENTER | Montreal, QC · 2023 · 264-unit building

Incident type	Coordinated break-and-enter — 8 units entered during engineered camera outage
Duration	Single 4-hour window; planning period estimated 3–4 weeks
Estimated loss	$211,000 in valuables; 3 residents present during entries — emotional distress claims filed
How detected	Residents reporting break-ins the following morning
Vulnerability root	Broadcast storm triggered intentionally by inserting a looped cable; no network resilience

INCIDENT NARRATIVE

At approximately 11:15pm on a Saturday in November 2023, every networked system in a 264-unit residential tower in Montreal's Plateau-Mont-Royal neighbourhood went offline simultaneously. Cameras stopped recording. The access control system lost its network connection. The security desk workstation crashed. Within moments of the outage, the physical door locks defaulted to their fail-open configuration — a setting that had never been reviewed or changed from the installer's default — and held that state until the network was restored at approximately 3:20am.

The cause of the outage was deliberate. Investigators later determined that an individual — believed to have had prior knowledge of the building's network setup — had inserted a looped patch cable into two ports on an unmanaged switch accessible in an unlocked electrical room on the ground floor. The loop created a broadcast storm that overwhelmed every switch in the building within seconds, taking all networked systems offline. The perpetrators — believed to be a group of four — then entered the building through a side door that had defaulted to unlocked and systematically entered 8 suites on floors 4 through 7, spending approximately 20 minutes per unit.

Three residents were present during the entries. None were physically harmed, but all three filed emotional distress claims against the corporation, arguing that the building's failure to secure network infrastructure had directly enabled a situation where strangers entered occupied residences. The corporation's liability insurer conducted its own investigation and identified the unlocked electrical room, unmanaged switches, and fail-open door configuration as material contributing factors. Coverage was paid but the corporation received notice that renewal would require evidence of remediation.

VULNERABILITIES EXPLOITED

- Unmanaged switches with no loop protection — single patch cable caused building-wide broadcast storm
- Electrical room with network equipment physically unlocked — accessible to any building visitor
- Access control system defaulted to fail-open — all doors unlocked during network outage
- No network resilience — no managed switching, no STP, no redundant path to maintain door control
- No UPS on network switches — power fluctuation during storm cascaded full system failure
- No out-of-band monitoring — management unaware of outage for over 4 hours

LESSON: Access control systems must be configured fail-secure (doors lock, not open, during network loss). All network equipment rooms must be locked at all times — a deadbolt, not just a wedge. Managed switches with Spanning Tree Protocol eliminate the broadcast storm attack vector entirely. This incident was entirely preventable with three configuration changes that cost nothing.

INC-007

The Management Office Walk-In

HIGH | FRAUD | Edmonton, AB · 2024 · 198-unit building

Incident type	Identity theft and financial fraud — resident personal data harvested from unsecured office
Duration	Believed to be a single 12-minute visit; fraud activity spanned 3 months afterward
Estimated loss	$43,500 across 6 affected residents (credit fraud, fraudulent lease applications)
How detected	Resident flagged unknown credit inquiry; police investigation linked to building visit
Vulnerability root	Management office freely accessible; resident files physically visible on desk; no visitor log

INCIDENT NARRATIVE

On a Tuesday morning in March 2024, an individual visited the management office of a 198-unit building in Edmonton's Oliver neighbourhood, claiming to be from a pest control company conducting a routine inspection. The property manager was alone, received a brief phone call, and stepped into the adjacent photocopier room for approximately 12 minutes while the visitor waited — as the manager later described it — 'just in the doorway.'

The visitor was not in the doorway. CCTV footage from a camera in the hallway showed the individual move directly to the manager's desk, photograph several open resident files with a phone, access the manager's unlocked workstation, and photograph the screen — which displayed a resident roster in the building's property management software. They were back in the doorway before the manager returned.

Over the following three months, six residents received notifications of fraudulent credit applications, unknown credit inquiries, and in two cases, fraudulent rental applications submitted in their names to other buildings in the city. The data harvested in those 12 minutes — names, unit numbers, date of birth from lease files, and the property management software interface — was sufficient to construct convincing identity profiles.

Police identified the individual through the hallway camera footage but were unable to locate them. The building had no visitor log, no pest control vendor on contract, and no record of the visit. The corporation faced six privacy complaints under PIPEDA and was required to submit a mandatory breach report to the Office of the Privacy Commissioner.

VULNERABILITIES EXPLOITED

- Management office freely accessible — no controlled entry, no visitor log, no ID verification
- Resident files physically open on desk — sensitive personal data visible to anyone in the room
- Unlocked workstation with resident data displayed — no screen lock, no timeout policy
- No vendor verification process — anyone claiming to be a contractor was admitted without confirmation
- Clean desk policy absent — sensitive documents not secured when staff were away from desk

LESSON: PIPEDA requires that personal information be protected against unauthorised access. A visitor log, an ID verification requirement, and a clean desk policy cost nothing to implement and would have prevented this entirely. Screen lock timeout of 3 minutes is a one-click Windows policy. Resident files must never be left open on an unattended desk.

INC-008

The Broadcast Storm Assault

CRITICAL ASSAULT Hamilton, ON · 2023 · 142-unit building

Incident type	Physical assault inside building during engineered camera and access control outage
Duration	Network outage lasted 22 minutes; assault occurred 7 minutes into outage
Outcome	Victim hospitalised — serious injuries. Perpetrator identified through witness accounts only; no camera evidence
How detected	Resident called 911 from suite; network restored before police arrival
Vulnerability root	Network loop in Telco room caused broadcast storm; cameras and access control failed simultaneously
Civil proceedings	Corporation named in negligence claim — matter ongoing at time of publication

INCIDENT NARRATIVE

At 9:47pm on a Friday in October 2023, all networked systems in a 142-unit lowrise in Hamilton went offline. Cameras stopped. The access control system dropped. The security desk workstation lost network. The on-duty concierge, unfamiliar with the system, assumed it was an internet outage and did not call management or initiate any emergency protocol — there was no written procedure for this scenario.

Seven minutes into the outage, a resident in the third-floor corridor was assaulted by an individual later described by witnesses as having followed them into the building through the main lobby door, which had been held open by a food delivery driver. With cameras offline and the access control system unable to record entry events, there was no electronic record of the perpetrator's entry, movement, or exit.

The network outage was caused by a pre-existing switching loop in the building's Telco room — a condition that had been causing intermittent partial outages for several months, which management had attributed to the ISP and never properly investigated. On this occasion, the loop triggered a full broadcast storm that overwhelmed every switch on the network. The 22-minute outage resolved itself when a switch powered down and rebooted automatically, breaking the loop.

Police charged a suspect based on witness descriptions and partial footage from a resident's personal doorbell camera in the stairwell. The building's own camera system provided nothing. The victim's legal counsel named the corporation in a negligence claim, arguing that the known network instability — evidenced by months of incident reports — and the absence of emergency procedures had created conditions that directly impaired the building's ability to protect residents.

VULNERABILITIES EXPLOITED

- Active switching loop in Telco room — broadcast storm took all security systems offline simultaneously
- No emergency procedure for network/camera outage — concierge had no protocol to follow
- Months of known instability never properly investigated — root cause never identified
- No out-of-band alert system — management unaware of outage until police arrived
- Fail-open configuration on lobby door — tailgating entry during outage went unrecorded
- All life-safety systems on single flat network — one failure point disabled everything

LESSON: A network loop is not just an IT problem — it is a life-safety risk. Any building experiencing intermittent unexplained outages should treat it as an emergency and commission an infrastructure audit immediately. Concierge staff must have a written procedure for camera or access control system failure — including who to call and what to do in the first 5 minutes.

INC-009 The Dealer in 1204

MEDIUM | DRUG TRAFFICKING | Toronto, ON · 2024 · 340-unit building

Incident type	Residential drug distribution — operation sustained by cloned common-area fobs issued to buyers
Duration	Approximately 5 months
Estimated scale	Police estimate 30–40 buyers per week accessing building; cocaine and MDMA distribution
How detected	Multiple resident complaints; police surveillance; review of access log anomalies
Vulnerability root	Cloneable 125kHz fobs; no audit of active credentials; no alert for high-frequency access events

INCIDENT NARRATIVE

Residents on the 12th floor of a 340-unit tower in Toronto's Liberty Village neighbourhood began complaining in mid-2024 about unusual foot traffic — unfamiliar individuals in the corridors at all hours, an elevator that seemed to run constantly to floor 12, and a persistent smell in the hallway near unit 1204. After several formal complaints, the property manager reviewed the building's access logs for the 12th-floor elevator lobby reader and found that on the previous Thursday alone, it had recorded 67 access events between the hours of 6pm and 2am. The next highest day in the prior month had 14.

Police were notified and executed a search warrant on unit 1204. The tenant — who had a legitimate lease — had been running a distribution operation from the unit for approximately five months. A key element of the operation was access: the tenant had been issuing cloned fobs to regular buyers, allowing them to enter the building independently without buzzing through the concierge. The fobs were cloned from a legitimate common-area fob that the tenant had obtained from a previous resident.

The building's access control system had no credential velocity alerting — no mechanism to flag when a single credential was used more than a threshold number of times in a given period. The 67 accesses in a single evening had generated no alert whatsoever. The management team only found the anomaly because they manually searched logs following resident complaints — something they had never done proactively. Police identified over 200 individual access events attributed to the cloned credential family across the 5-month period.

VULNERABILITIES EXPLOITED

- 125kHz fob technology — cloneable in seconds, distributed to third parties with no detection
- No credential velocity alerting — 67 accesses in one evening triggered zero system response
- No proactive audit log review — anomaly only discovered after sustained resident complaints
- No duplicate credential detection — cloned UIDs registered identically to original
- Common-area fob used as master key — single cloned fob gave access to all shared spaces

LESSON: Access control systems should be configured to alert management when any single credential exceeds a configurable threshold of uses per day (e.g. more than 10 accesses in 24 hours). This single configuration change would have flagged this operation within its first week. Weekly log review — even a 5-minute scan for statistical outliers — is a free mitigation.

INC-010 The Printer Harvest

HIGH | PRIVACY BREACH | Winnipeg, MB · 2023 · 224-unit building

Incident type	Mass privacy breach — resident personal data exfiltrated from management office printers
Duration	Estimated 3–4 weeks of active data collection
Scale	Personal data of approximately 180 residents compromised — names, SINs, bank details from lease applications
How detected	Residents began receiving targeted phishing calls 6 weeks after incident
Vulnerability root	Printers on flat LAN with default admin credentials; print job storage enabled; accessible from any network device

INCIDENT NARRATIVE

In late 2023, residents of a 224-unit building in Winnipeg's Exchange District began receiving highly targeted phone calls from individuals claiming to be from their bank, referencing specific financial details that the callers could only have known from the residents' original rental applications — including partial SIN numbers, employer names, and monthly income figures. Eleven residents reported the calls before one of them — a cybersecurity professional — connected the pattern to their building.

A review of the building's network found that its three management office printers were connected to the same flat LAN as all other building systems, including resident Wi-Fi. Each printer had a web-based admin interface accessible from any device on the network, and all three were still operating with factory-default administrator credentials. All three were also configured with print job storage enabled — meaning every document printed in the management office was retained in the printer's internal memory and accessible through the admin interface.

An individual who had accessed the building's Wi-Fi — potentially during a visit as a prospective resident, a contractor, or a delivery person — had discovered the printers on the network, accessed their admin interfaces using the default credentials, and downloaded the stored print job queue. The queue contained approximately 180 lease applications, renewal letters, and resident financial documents that had been printed over the previous 14 months. The data was later used to construct phishing profiles targeting the affected residents.

The corporation filed a mandatory privacy breach report with the Office of the Privacy Commissioner. It subsequently received notification from 11 residents of financial losses totalling approximately $31,000 attributed to the resulting fraud. The matter was referred to the RCMP Cybercrime unit.

VULNERABILITIES EXPLOITED

- Printers on flat LAN accessible from guest and resident Wi-Fi — no network isolation
- Factory-default admin credentials on all three printers — never changed since installation
- Print job storage enabled — 14 months of sensitive resident documents stored in printer memory
- No network segmentation — Wi-Fi guest access shared broadcast domain with management systems
- No printer security policy — no awareness that printers retain and serve print history

LESSON: Printers are network computers. They must be on an isolated management VLAN, have admin credentials changed from default, and have print job storage disabled. Any printer that has been on an unsegmented network should be treated as potentially compromised and its print history cleared immediately. This incident would have been prevented by a $0 configuration change made on day one of printer installation.

INC-011

The Fake Delivery Ring

MEDIUM | THEFT | Brampton, ON · 2024 · 288-unit building

Incident type	Organised theft ring posing as delivery drivers — 34 package thefts plus 6 suite entries
Duration	Approximately 13 weeks
Estimated loss	$78,000 including package thefts, stolen items from suites, and one vehicle theft
How detected	Resident recognised repeat 'driver' — reported to management and police
Vulnerability root	No delivery management system; concierge social engineering; camera footage retained for only 5 days

INCIDENT NARRATIVE

Over a 13-week period beginning in January 2024, residents of a 288-unit building in Brampton experienced a sustained pattern of package theft and, in six cases, the theft of items from inside suites. The operation was run by a rotating group of individuals who presented themselves to the concierge as delivery drivers from various courier services — some genuine, some fictional — and were consistently admitted to the building to 'make their delivery.'

Once inside, the individuals would collect packages from the lobby parcel shelf, but in several cases they were observed on personal dashcam footage entering elevator corridors and, on one occasion, entering a suite whose resident had left the door ajar while bringing in groceries. The concierge had no procedure for verifying delivery driver identity, no list of approved courier companies, and no system for logging deliveries or tracking who had been admitted to the building.

When residents began raising concerns, management attempted to review camera footage but discovered the NVR was configured to retain footage for only five days before overwriting — a setting that had been the default since installation and had never been changed. By the time the pattern was recognised, all footage predating the most recent five days was gone. Police were therefore unable to obtain footage covering the vast majority of the incident period and the investigation stalled.

VULNERABILITIES EXPLOITED

- No delivery verification procedure — any person claiming to be a courier was admitted without ID check
- NVR retention set to 5 days — critical footage overwritten before pattern was recognised
- No delivery management system — no log of who was admitted, for what purpose, or when
- Concierge social engineering — confident presentation as a courier was sufficient for entry
- No alert for unusual concierge-admitted visitor frequency — no one noticed the volume of 'deliveries'

LESSON: Camera retention must be a minimum of 30 days — this is a one-click NVR configuration change provided storage is sufficient. Concierge procedure must include a simple delivery verification protocol: accepted couriers are logged, unrecognised individuals are asked to leave packages in the lobby and not proceed past the front desk. This does not require technology — just policy.

INC-012 The Insider Wipe

CRITICAL | VANDALISM | Vancouver, BC · 2024 · 376-unit building

Incident type	Deliberate sabotage — access control and camera databases wiped by disgruntled former contractor
Duration	Single remote session lasting approximately 40 minutes
Recovery cost	Estimated $118,000 in system restoration, credential re-enrollment, and interim security staffing
How detected	Access control system began rejecting all credentials simultaneously at 11:38pm
Vulnerability root	Former contractor retained admin credentials to access control and camera systems; no backup; no MFA on remote access

INCIDENT NARRATIVE

At 11:38pm on a Wednesday in February 2024, the access control system at a 376-unit highrise in Vancouver's Coal Harbour neighbourhood stopped accepting all credentials simultaneously. Every fob in the building — resident, staff, contractor, and master — was rejected. Doors defaulted to fail-open. The security desk alerted management, who contacted the access control vendor's emergency line. By the time a technician connected remotely to diagnose the issue, the damage was done: the entire credential database had been wiped. Every resident record, every access level, every audit log — gone.

Forensic analysis of the system logs — recovered partially from a cached temp file — identified that an admin-level remote session had been initiated at 11:21pm from an IP address subsequently traced to a café in Burnaby. The session had accessed the access control server using credentials belonging to a technology contractor whose engagement with the building had ended eight months earlier following a payment dispute with the property management company.

The contractor had retained their admin login to both the access control server and the camera management system. In the same session, they had deleted all camera recordings from the previous 90 days and factory-reset the NVR. There was no backup of the access control database. There was no backup of the camera footage. There was no MFA on either system's remote access interface. The corporation spent approximately 12 days re-enrolling credentials manually from paper records, during which building security relied entirely on physical security guards stationed at every entry — at a cost of approximately $8,400 per day.

The contractor was charged with mischief over $5,000 and unauthorised use of a computer system. The total recovery cost — including system restoration, emergency security staffing, legal fees, and the access control vendor's emergency rebuild — exceeded $118,000. The building's insurer covered approximately $70,000 of that amount. The remainder was a reserve fund draw that required a special assessment.

VULNERABILITIES EXPLOITED

- Former contractor admin credentials never revoked — 8 months of post-contract access to critical systems
- No MFA on access control or camera system remote access — static password was sufficient for full admin entry
- No database backup — access control credential database had never been backed up
- No camera footage backup — 90 days of recordings deleted with no recovery path
- No session monitoring or anomaly alerting — 40-minute admin session at midnight triggered no alert
- No IT off-boarding checklist — credential revocation was not a documented step in contractor termination

LESSON: This incident — costing over $118,000 and requiring a special assessment — would have been prevented by two actions: revoking the contractor's credentials on their last day, and maintaining a weekly database backup stored offline. MFA on any system with destructive admin capabilities is non-negotiable. No credential should survive a contract ending — not a fob, not a login, not a remote access session.

Incident Summary — All 12 Cases

ID	Title	Category	City	Loss/Impact	Sev.
INC-001	The Cloned Fob Ring	Theft	Toronto, ON	$187,000	HIGH
INC-002	The Dark Web Drone Drop	Drug Trafficking	Vancouver, BC	$340,000+	HIGH
INC-003	The Invisible Stalker	Stalking	Ottawa, ON	Criminal	CRIT
INC-004	The Parking Garage Strippers	Theft / Vehicle	Calgary, AB	$94,000	HIGH
INC-005	The Superintendent's Backdoor	Fraud	Mississauga, ON	$62,000	CRIT
INC-006	The Camera Blackout Burglaries	Break & Enter	Montreal, QC	$211,000	HIGH
INC-007	The Management Office Walk-In	Fraud / ID Theft	Edmonton, AB	$43,500	HIGH
INC-008	The Broadcast Storm Assault	Assault	Hamilton, ON	Civil claim	CRIT
INC-009	The Dealer in 1204	Drug Trafficking	Toronto, ON	Criminal	MED
INC-010	The Printer Harvest	Privacy Breach	Winnipeg, MB	$31,000+	HIGH
INC-011	The Fake Delivery Ring	Theft	Brampton, ON	$78,000	MED
INC-012	The Insider Wipe	Sabotage	Vancouver, BC	$118,000	CRIT

Common Vulnerability Patterns Across All 12 Incidents

Vulnerability	Appears in	Notes
Cloneable credentials (125kHz)	INC-001, 009	9 of 12 incidents — most prevalent single vulnerability
No network segmentation	INC-002, 003, 006, 010	Cameras, access control, office on same LAN
Default passwords unchanged	INC-002, 005, 010, 012	Factory credentials in place for months or years
No credential off-boarding	INC-003, 005, 012	Contractor/staff access persisting after termination
Failed or missing UPS	INC-004, 006, 008	Power failure cascaded to camera and access outage
No audit log review	INC-001, 008, 009	Anomalies undetected for weeks or months
No camera footage backup	INC-002, 011, 012	Single-point storage with no offsite redundancy
Short retention period	INC-004, 011	Footage overwritten before investigation commenced
No MFA on remote access	INC-005, 012	Static password sufficient for full system admin
Physical access to network gear	INC-006, 007	Unlocked equipment room or accessible management office

IMPORTANT NOTICE: All 12 incidents described in this document are entirely fictional and created for illustrative and educational purposes only. They are designed to demonstrate the real-world consequences of security vulnerabilities commonly identified during Mycondolink technology audits of residential condominium properties in Canada. No real buildings, residents, corporations, police forces, or insurers are referenced. Any resemblance to actual events is coincidental. This document is intended exclusively for Board presentations, property manager education, and audit proposal support.