Cybersecurity Best Practices & Breach Response Strategies

Mouna Hanna
Partner, Canadian Head of Cyber,
Privacy & Data Protection Group

dwfgroup.ca

Western
UNIVERSITY · CANADA

The Legal Stuff

The information shared is for general informational purposes and does not constitute legal advice. Each cyber incident is different, and we encourage you to seek counsel before you make any decisions or take any action during a cyber incident.

Who We Are

- Five offices in Canada: Vancouver, Victoria, Calgary, Toronto & Montreal

- Over 160 lawyers across Canada

- Breach Response Services
  - Breach coach
  - Funds tracing and recovery following wire fraud

- Pre-Breach/Risk Management Services
  - Incident response plans
  - Tabletop exercises

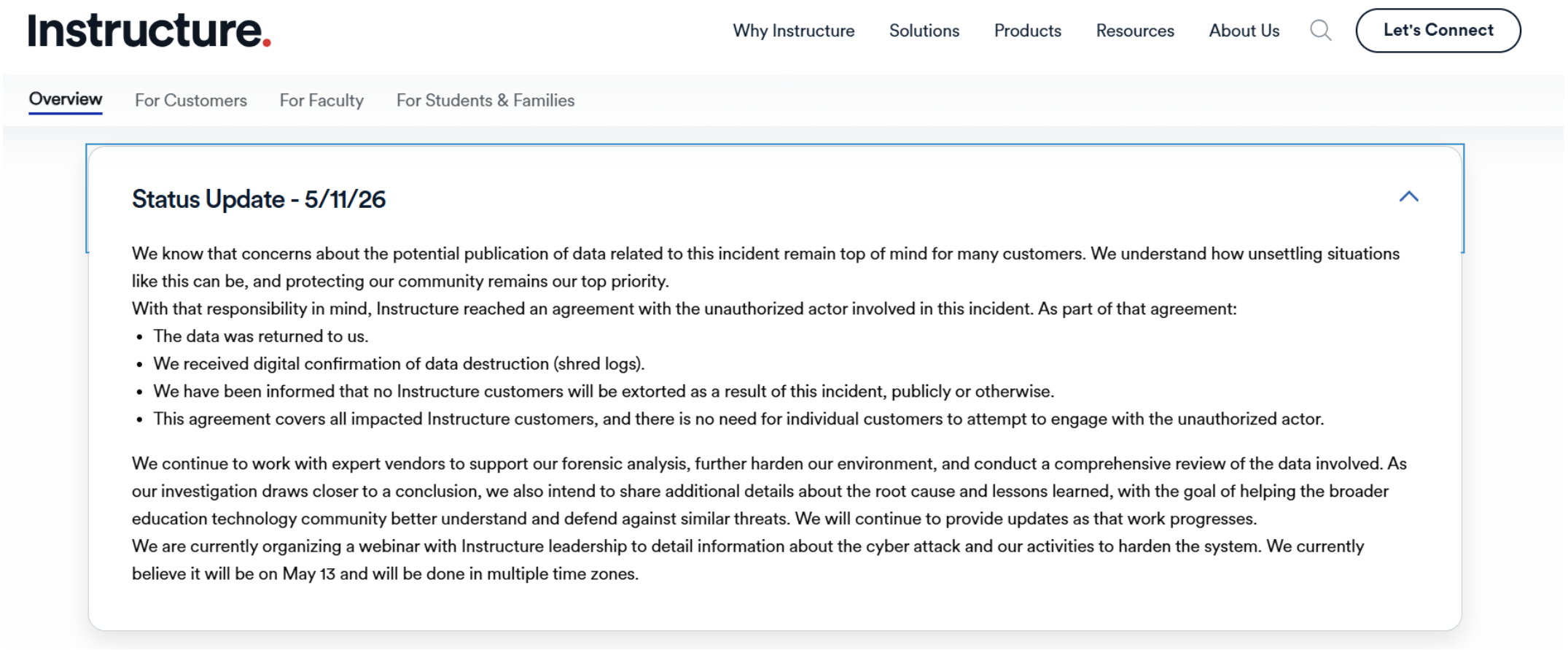
- Post-Breach Litigation
  - Civil and regulatory defence post data breach
  - Defence of professional negligence claims

In The News

Canvas (Infrastruture) Breach – April, 2026

- ShinyHunters – Threat Actor Group
- Exploited a vulnerability within the Free-For-Teacher product and claimed to have stolen/exfiltrated 3.65 TB of data across approximately 275 million records from 8,809 educational institutions
- When Infrastructure did not engage, the TA named Infrastructure on its leak site on the dark web and defaced approximately 330 Canvas school login portals to exert pressure
- The TA removed Infrastructure from the leak site
- The TA then targets individual schools

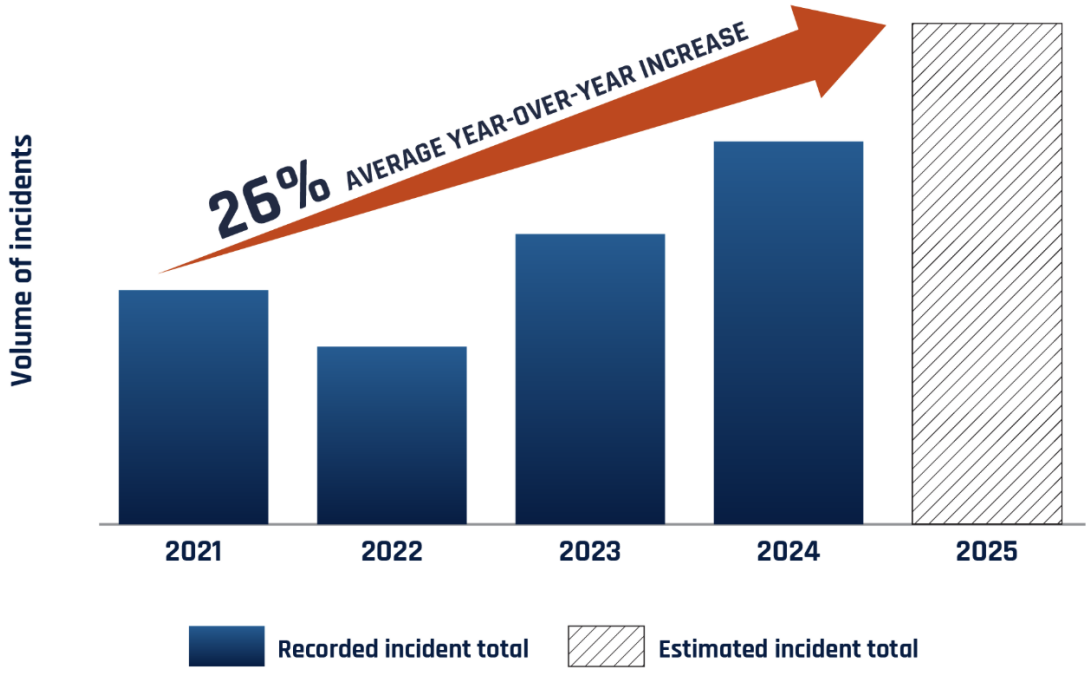
In The News


Instructure.
Why Instructure
Solutions
Products
Resources
About Us
Let's Connect
Overview
For Customers
For Faculty
For Students & Families
Status Update - 5/11/26
We know that concerns about the potential publication of data related to this incident remain top of mind for many customers. We understand how unsettling situations like this can be, and protecting our community remains our top priority.
With that responsibility in mind, Instructure reached an agreement with the unauthorized actor involved in this incident. As part of that agreement:
• The data was returned to us.
• We received digital confirmation of data destruction (shred logs).
• We have been informed that no Instructure customers will be extorted as a result of this incident, publicly or otherwise.
• This agreement covers all impacted Instructure customers, and there is no need for individual customers to attempt to engage with the unauthorized actor.
We continue to work with expert vendors to support our forensic analysis, further harden our environment, and conduct a comprehensive review of the data involved. As our investigation draws closer to a conclusion, we also intend to share additional details about the root cause and lessons learned, with the goal of helping the broader education technology community better understand and defend against similar threats. We will continue to provide updates as that work progresses.
We are currently organizing a webinar with Instructure leadership to detail information about the cyber attack and our activities to harden the system. We currently believe it will be on May 13 and will be done in multiple time zones.


[AKIRA]
AKIRA
Well, you are here. It means that you're suffering from cyber incident right now. Think of our actio
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a
fair price to make it all go away.
Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow o
ur instructions to get back to your daily routine, by cooperating with us you will minimize the dama
ge that might be done.
Those who choose different path will be shamed here publicly. The functionality of this blog is extr
emely simple - enter the desired command in the input line and enjoy the juiciest information that c
orporations around the world wanted to stay confidential.
Remember. You are unable to recover without our help. Your data is already gone and cannot be traced
to the place of final storage nor deleted by anyone besides us.
guest@akira:~$ help
List of all commands:
leaks — hacked companies
news — news about upcoming data releases
contact — send us a message and we will contact you
help — available commands
clear — clear screen
guest@akira:~$

Ransomware: Still a Problem

Figure 1: Growth from 2021 of Canadian ransomware incidents known to the Cyber Centre



Source: Ransomware Threat Outlook 2025-2027 - Canadian Centre for Cyber Security

2026 Ransomware Trends

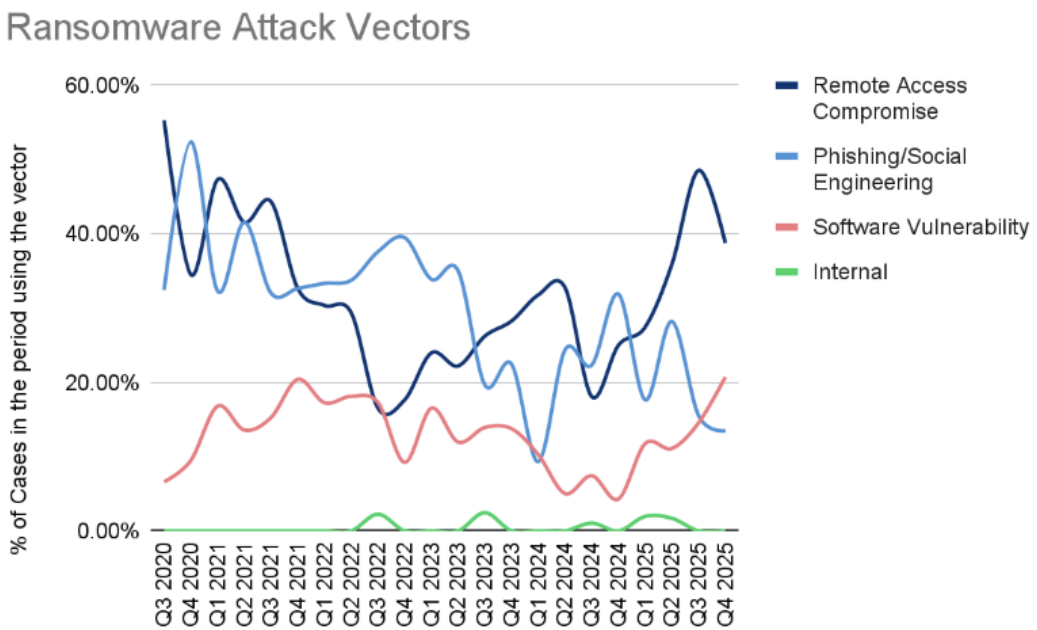
In The Trenches

- Fewer victims paying overall
  - Better prepared
  - Volatility and “distrust” re threat actors
  - But trend is **not** due to a reduction of threat activity
- Increased number of attacks by “unaffiliated” actors or lone wolves
- More aggressive negotiation tactics and uncharacteristic behaviour
- Top attack vectors: remote access compromise/firewall compromise
  - MFA bypass/MFA fatigue
- Threat actors using legitimate file transfer tools to move data out of the environment - undetected
  - Ie. Seafile, dropbox

2026 Ransomware Trends

In The Trenches

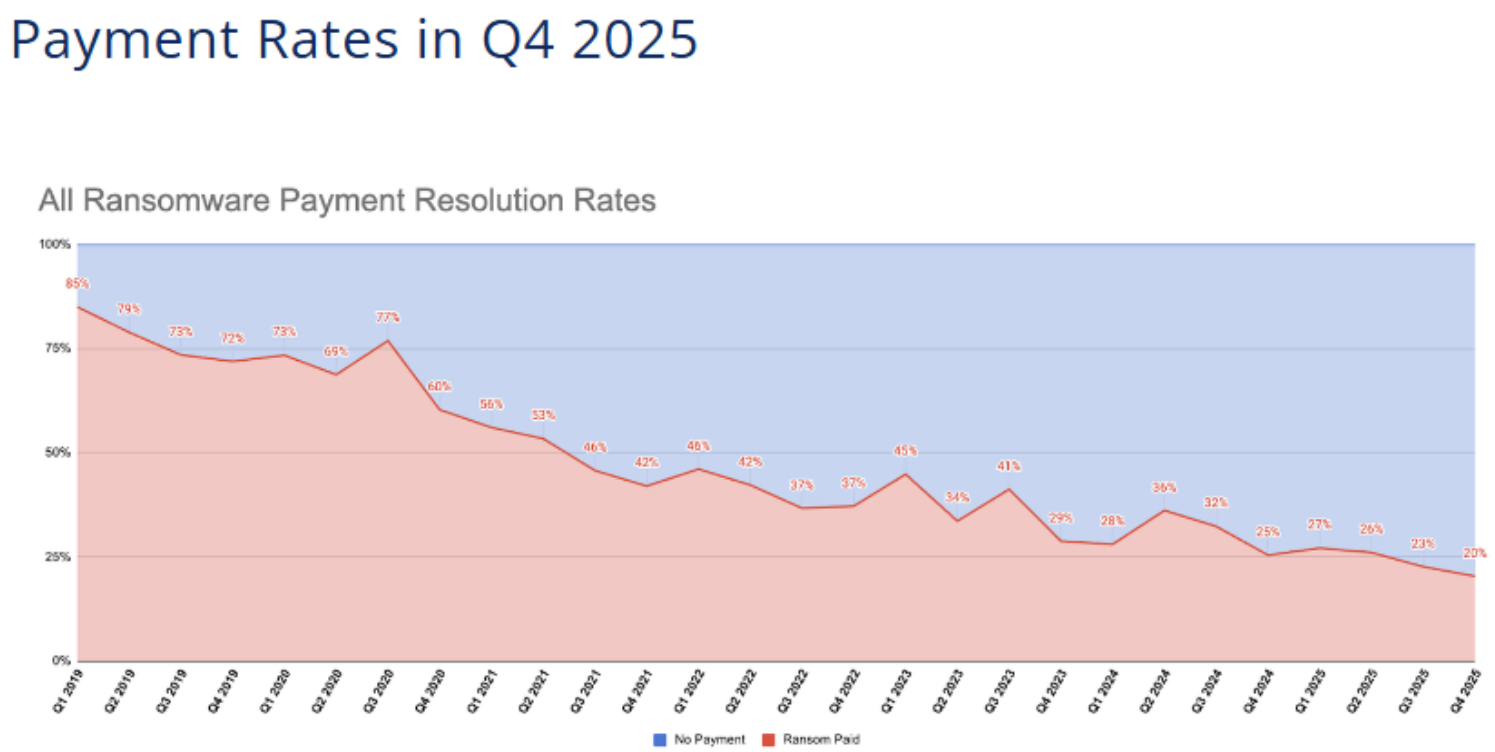
Most Common Initial Attack Vectors in Q4 2025



Source: Coveware

2026 Ransomware Trends

In The Trenches



Source: Coveware

Common Cyber Related Attacks

In The Trenches

- Cybersecurity Breaches
  - Ransomware, software vulnerabilities, data theft, business email compromise, malicious URLs, bug bounty hunters
- Wire fraud
  - Social engineering/phishing, “man in the middle attacks”, manipulated invoices and “updated banking information”
- Inadvertent Disclosure of Personal Information
  - Employee error, theft or misconduct, loss of a device

Higher Education/EdTech

Remains a top target

- Massive volume of data
  - Personal information of students and faculty
  - IP/proprietary research and data
- Heavy reliance on third party shared platforms and cloud software with no visibility or true control over security protocols
- Device targets/BYOD on campus heightens risk
- Constrained cybersecurity/IT budgets
- Cannot afford operational downtime – perceived pressure for institutions to pay quickly to regain access to IT systems

FIPPA/PHIPA

IPC Guidance for Breach Response

FIPPA

- Assess the scope of the breach and contain it
- Assess whether the privacy breach creates a **real risk of significant harm (RROSH)** to the affected individual(s)
- Notify those affected by the breach where it is reasonable to believe there is a RROSH and report the breach to the IPC
  - Mandatory breach notification effective July 1, 2025
- Investigate the breach to identify and analyze key facts, events, and issues that contributed to it
- Take measures to reduce the risk of future privacy breaches

PHIPA

- May apply where the affected data is personal health information in the custody or control of a health information custodian affiliated with the institution (for example, certain clinic operations)

Notification & Reporting

RROSH

- “real risk” – more than mere speculation or conjecture
- “significant harm” – bodily harm, humiliation, damage to reputation or relationships, financial harm, identity theft, phishing etc.
- Low threshold
- Reporting to Ontario’s Information and Privacy Commissioner
- No strict timeline for notification and reporting – as soon as reasonably possible after determining that a privacy breach has occurred

Breach Response

It all starts with a scoping call

- Coordinated through a ‘Breach Coach/Breach Counsel”
- Activate incident response plan and bring together relevant stakeholders
- Engage data forensic/incident response vendors (through counsel) to:
  - Contain the breach
  - Isolate any affected systems
  - Remove any ongoing threats or vulnerabilities
  - Assess the scope of the breach and data at risk
- Develop a communication plan and strategy
- Legal obligations and regulatory compliance
- Engage law enforcement
- Minimize potential harm/exposure and liability

Looking Ahead – Risk Mitigation

Consider

- Data Minimization
- Protecting data, understanding where it is being stored and who has access to it
  - Consider encrypting sensitive data
  - Ensuring you have current and viable backup data
  - Ensuring third parties adequately protect your data in their possession by conducting regular audits and understanding potential exposures arising from downstream risks
- Develop and test your incident response plan
  - Consider holding statements, communication strategies and out of band contact information for key stakeholders
- Creating a cyber-aware culture with ongoing training

Questions?

DWF is a leading global provider of integrated legal and business services.

Our Integrated Legal Management approach delivers greater efficiency, price certainty and transparency for our clients.

We deliver integrated legal and business services on a global scale through our three offerings; Legal Services, Legal Operations and Business Services, across our nine key sectors. We seamlessly combine any number of our services to deliver bespoke solutions for our diverse clients.

dwfgroup.ca