ZURICH
Brandschenkestrasse 24
CH-8027 Zurich

GENEVA
Route de Chêne 30
CH-1211 Geneva 6

LAUSANNE
Avenue de Rhodanie 40C
CH-1007 Lausanne

Cyber Threats Briefing Summary

Lenz & Staehelin in partnership with Toro Solutions, recently hosted a cyber threat briefing focused on the risks facing businesses and private clients and the strategies they should consider to improve resilience. With the cost and frequency of cyber attacks continuing to rise, the gap between threat awareness and practical preparedness is growing. With the proliferation and increasing capabilities of AI systems, the risks and threat levels are rising rapidly. Attacks happen every day, and too many organisations are still on the back foot. This short article outlines the key points addressed during the threat briefing by Toro's Founder and CEO Peter Connolly and Lenz & Staehelin Partner Fedor Poskriakov.

Published: 6 June 2025

EXPERTISE Private Clients

Why now?

Peter opened with a stark set of statistics illustrating the current cyber threat landscape:

- Cybercrime is estimated to global cybercrime costs to grow by 15% per year over the next five years, reaching $10.5 trillion USD annually by 2025
- 7% of businesses experienced financial or data loss last year
- 56% of organisations still lack a formal incident response plan
- On average, it takes 255 days to detect a breach
- The typical cost of a cyber incident now exceeds CHF 2 million

Peter's message was simple: it's not a question of *if* a business will be targeted, but *when*. And when it happens, not having a tested response plan can do more damage than the attack itself.

Ransomware - A persistent & profitable threat

Ransomware remains one of the most common and costly incidents:

- It accounts for 24% of all breaches
- Incidents rose by 13% last year
- Insurers will pay the full ransom in only 1% of cases. In 79% of cases, the insurer funded less than half of the total payment.
- Of those, nearly a third had to pay more than once
- Even after payment, only 68% of data was fully recovered

The rise of ransomware-as-a-service has lowered the barrier to entry. Sophisticated tools are now widely available to criminal groups and opportunists alike. Yet, many organisations still lean on cyber insurance or assume they won't be a target. As Peter and Fedor pointed out, that's not a plan. Preparation is critical – from purely technological, to governance and training – a number of sometimes simple steps help manage the risks of cyber attacks.

The rise of blended attacks

Peter explained how today's security threats rarely come in isolation. More and more, we are seeing blended attacks – where attackers use a combination of technical breaches, social engineering, online and physical reconnaissance. By combining these tactics, criminals are exploiting the path of least resistance, using whatever vulnerabilities are easiest to access whether that's a physical security gap, a human error, or a technical weakness.

To illustrate this, Peter shared a real-world example showing how attackers can use publicly available information such as social media profiles, contact directories, and breached credentials to build a detailed picture of their targets.

Once inside, attackers often focus on:

- Compromising business email systems to intercept payments
- Exploiting weak backup and disaster recovery processes
- Targeting staff through phishing and impersonation

Many organisations still treat cyber, physical, and their people as separate disciplines whereas Peter showed that in reality, attackers don't respect those boundaries. A weak physical process, an overlooked email rule, or a delayed legal response can all lead to the same outcome: data loss, reputational damage, and financial impact.

The most resilient organisations are the ones that bring together their cyber, physical, technical, legal, and operational teams to plan, prepare, and respond as one.

Managing the risks of your Digital Footprint

Every online action from a LinkedIn update to an embedded metadata tag in a PDF contributes to your organisation's digital footprint. This includes:

- Public-facing employee profiles
- Company websites, news articles, and press releases
- Job ads that disclose internal tools or team structures
- Breached credentials from third-party leaks
- Cloud infrastructure meta data (e.g., exposed IPs)

While much of this data may seem harmless, threat actors **connect minor, seemingly harmless details** to launch highly targeted attacks.

In more severe cases, this online exposure can lead to real-world risks, such as:

- Surveillance or physical intrusion based on mapped routines
- Social engineering attacks using personal and organisational data
- Executive targeting, particularly in sectors like finance or crypto
- Reputational attacks using resurfaced or manipulated content

This isn't limited to advanced actors. Even low-sophistication criminals can use freely available tools and OSINT (open-source intelligence) methods to impersonate staff, register spoofed domains, or hijack conversations for fraud.

What you can do now

While the threat landscape is evolving, the fundamentals of good security remain the same. Peter and Fedor shared some immediate steps any organisation can take:

Get the basics right

- Use strong, unique passwords and enable multi-factor authentication
- Keep software and firmware up to date
- Review and secure remote access and VPN settings
- Implement regular patching cycles

Understand your exposure

- Audit your digital footprint and reduce unnecessary public data
- Know your attack surface and monitor it continuously
- Assess supply chain risks and third-party access

Build and test a response plan

- Create and test a formal incident response plan
- Ensure you have working, offline backups
- Regularly test disaster recovery procedures to ensure you can restore critical services

Train your people

- Run regular phishing simulations
- Make sure staff know how to report suspicious activity
- Build a culture of security awareness at all levels
- Don't just train your people, test them

Include legal in your security planning

- Understand your obligations under data protection and cyber incident reporting laws in all jurisdictions in which you operate
- Involve legal counsel in response planning
- Establish clear roles for internal and external communications during an incident

Final thoughts

Cyber threats continue to evolve, but in many cases, it's the basics that still cause the most damage. Weak passwords, missed updates, poor processes are often the entry points.

The organisations that recover fastest aren't necessarily those with the most advanced technology. They're the ones who have established and tested their plans, trained their teams, and are clear on what to do on the day it happens on all aspects (i.e., technology, communication, legal, etc.).

To find out more, or to speak with our team about readiness assessments or legal risk planning, please get in touch with Toro Solutions or Lenz & Staehelin.

References:

- $10.5Tn pa: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
- 6.5% of businesses lost data/money last year: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024
- Ransomware insurance payouts: https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

CONTACTS	Fedor Poskriakov	Deputy Managing Partner, Head of Fintech, Genève fedor.poskriakov@lenzstaehelin.com Tel: +41 58 450 70 00
	Daniel Schafer	Deputy Head Private Clients, Genève daniel.schafer@lenzstaehelin.com Tel: +41 58 450 70 00
	Nathalie Vetsch-Cevallos	Partner, Lausanne nathalie.vetsch-cevallos@lenzstaehelin.com Tel: +41 58 450 70 00