SKURIO

The essential guide to

Digital Risk Protection

Protecting your products and services

skurio.com

Protect your goods and services

Almost every aspect of your business relies on data in one way or another.

Theft of intellectual property and strategic or confidential information can impact your products or services and pose a significant digital risk to your business.

According to Verizon, over 70% of workers admit taking intellectual property when they resign.

All businesses are data-driven — stop your best assets from being used against you

3 things bad actors look for

- Stolen or counterfeit goods and stolen gift cards/codes
- Unprotected repositories for sensitive documents
- Vulnerabilities in loyalty card schemes

3 ways they can use them against you

- Facilitate counterfeiting of your goods and services or handling stolen goods
- Disclosure of breached data to press, authorities or competitors
- Financial fraud or extortion activities

3 ways this increases digital risk

- **Operational:** jeopardised business strategy
- **Reputational:** unwanted media coverage
- **Financial:** loss of revenue and reduced ability to compete

Our customers agree...

> **"Skurio's keyword search and monitoring make it an ideal platform for us to use for external threat hunting, it's extremely flexible."**
>
> Mahir Mohsin Sheikh, Cydea Tech CEO and founder

Monitor for product and IP theft outside your network

You might not be able to stop all theft of your products or data critical to the manufacture or supply of your services, especially if it has taken place in your supply chain. But, if you can detect it, you can identify the cause and prevent further leaks or theft. More importantly, early detection will allow you to take measures that mitigate risk. Proactively using techniques like digital watermarking can help you pinpoint breaches even sooner.

Go beyond credential monitoring

- Use Digital Risk Protection to safeguard products, services, and intellectual property
- Add digital watermarks to verify if data found belongs to you and reduce false positives

4 easy ways to reduce risk

- Monitor for the sale of stolen or counterfeit goods
- Use security permissions to stop staff from downloading data
- Use unique digital watermarks to track any movement of intellectual property
- Request a takedown of publicly posted data

Close up

Critical business data breach

How your critical data is compromised

- **Account takeover:** previously breached staff credentials could allow criminals to access files or applications.
- **Supply chain attack:** vulnerabilities in your supply chain could put data at risk from remote access and exfiltration.
- **Insider threat:** whistle-blowers or aggrieved staff are willing to sell or leak data.
- **Accidental loss:** a misaddressed email or lost device that contains confidential information.

Details you can use to monitor for critical business data

- Company name, brand, and product names
- File headers and names
- Pattern match (REGEX) searching
- Data or code watermark
- Common intellectual property terms
- Staff names

Close up

Critical business data breach

Monitoring results you can expect to find

- Files posted in forums or dumpsites
- Content from email correspondence
- Exfiltrated data for sale on the Dark Web or dumpsites
- Counterfeit product listings on marketplaces

How bad actors use data to target your business

- **Disclosure:** bad actors leak breached data to the press, authorities, or competitors.
- **Counterfeiting:** confidential information helps criminals produce counterfeit goods.
- **Extortion:** fraudsters use sensitive data to blackmail your staff or business with the threat of disclosure.
- **Social engineering:** confidential details are used as bona fides indicators to coerce or manipulate your staff.

Steps you can take that reduce risk

- Trademark your brands and logos etc.
- Take steps to protect your intellectual property by filing patents
- Adopt a 'least privilege access model' to ensure only authorised staff can access important documents
- Watermark data to establish breach origination
- Request a takedown of information from the site
- Identify the source of the breach and mitigate against future risk

SKURIO

Close up

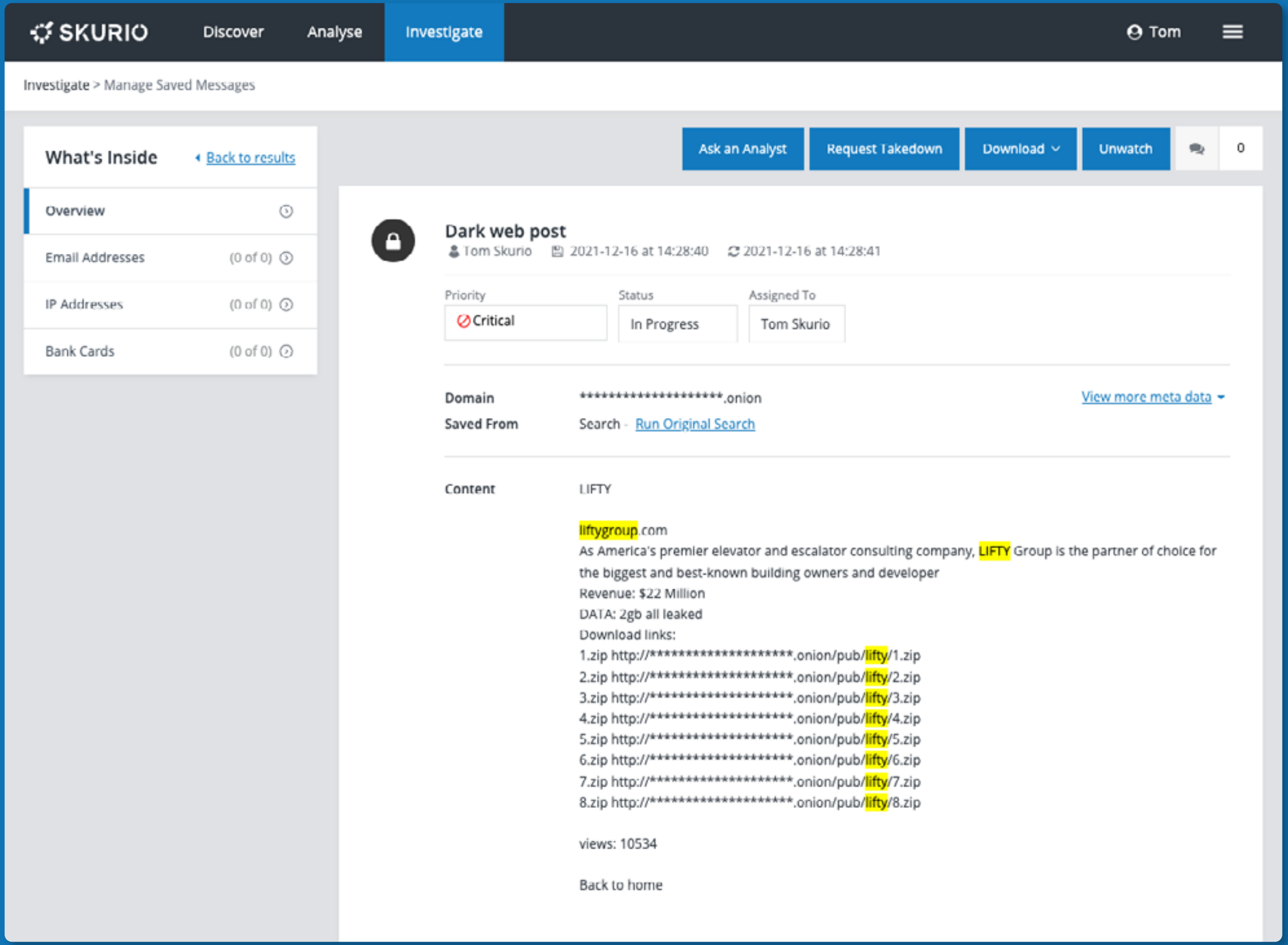
Critical business data breach

Sharing exfiltrated data on the Dark Web

This example shows corporate data posted on the Dark Web that is available freely for download.

The post may have resulted from data exfiltration following a supply chain attack or from non-payment of a ransomware attack. Note the high number of views on this post, which suggest the data could be in the hands of multiple cybercriminals.

DRP users can save any critical message and initiate an investigation. Investigations are assigned and prioritised, then team members can collaborate with comments as the investigation progresses.



Dark web post
Tom Skurio 2021-12-16 at 14:28:40 2021-12-16 at 14:28:41

Priority: Critical
Status: In Progress
Assigned To: Tom Skurio

Domain: ********************.onion
Saved From: Search - Run Original Search

View more meta data

Content:

LIFTY

liftygroup.com
As America's premier elevator and escalator consulting company, LIFTY Group is the partner of choice for the biggest and best-known building owners and developer
Revenue: $22 Million
DATA: 2gb all leaked
Download links:
1.zip http://********************.onion/pub/lifty/1.zip
2.zip http://********************.onion/pub/lifty/2.zip
3.zip http://********************.onion/pub/lifty/3.zip
4.zip http://********************.onion/pub/lifty/4.zip
5.zip http://********************.onion/pub/lifty/5.zip
6.zip http://********************.onion/pub/lifty/6.zip
7.zip http://********************.onion/pub/lifty/7.zip
8.zip http://********************.onion/pub/lifty/8.zip

views: 10534

Back to home

Use case samples represent real life examples. Data has been changed to protect the privacy organisations where appropriate.

Extended use cases

	Gift card sale Physical and digital gift cards are irresistible to criminals because they have a cash value but are virtually untraceable.	**Source code leak** Source code leaks can provide hackers with vital intelligence to help them gain access to critical systems or even change the code itself. If it gets into the hands of your rivals, you could potentially lose your competitive advantage.	**Loyalty schemes** Data breaches from loyalty cards or schemes are a hidden treasure for cyber-criminals. This data is often processed indirectly and may not have the same protection as datasets used for critical applications. Yet, customers often use the same credentials for both. As a result, criminals could take over customer accounts.
Details bad actors look for	• Unprotected gift card codes • Stolen cards • Staff that are willing to share codes	• Source code headers • Copyright markings •Code authors	• Unprotected databases • Supply-chain partners with more vulnerable access • Credential breaches for applications that handle loyalty scheme data
How they can be used	• Money laundering • Fraudulent purchase of goods	• Vulnerability exploitation • Sale of code to competitors • Active source code alteration • Code is shared publicly	• Monetised through Dark Web sales • Account takeovers • Phishing/Smishing • Social engineering
How this increases digital risk	• Loss of trust • Loss of revenue • Criminal investigation	• Reputational damage • Loss of competitive advantage • Compromised systems • Loss of intellectual property	• Loss of trust • Customer churn • Loss of revenue • Regulatory fine
Steps you can take	• Use DRP to monitor for gift card advertising with identified brands • Use text/numerical patterns (REGEX) in digital codes to improve traceability • Cancel cards promptly when a breach is detected	• Use DRP to monitor for source code headers, copyright markings and code authors • Identify the source of the leak • Request a takedown • Check code for modifications	• Use DRP to monitor for a subset of customer data or BreachMarker identities • Monitor for mentions of keywords used by your scheme • Identify and address the source of the leak • Notify customers and enforce a password reset

Skurio Digital Risk Protection

Skurio Digital Risk Protection provides you with the foundation necessary to adopt a data-centric approach to cybersecurity for your business.

Skurio continuously monitors the surface, deep and Dark Web for your data and instantly alerts you whenever it is found.

Skurio Cyber Threat Intelligence looks for cyber threats specific to your business, giving you a single view of all data protection incidents and threats outside your network. BreachMarker and BreachResponse features protect your data across your supply chain and integrate valuable alerts into your response management systems.

Dark Web Monitoring

- Monitor for staff, customer, infrastructure, and critical business data 24x7
- Tailored searches on social, surface, Deep and Dark Web sources
- Search years of historical data to know your digital footprint

Data Breach Detection

- Get instant alerts if your Skurio detects data outside your network
- Automate your breach response playbooks with readymade integrations to SIEM and ITSM systems
- Instantly identify the source of a breach with data-watermarking

Cyber Threat Intelligence

- Combine curated content relevant to your business to speed up investigations
- Use intuitive analytics to get usable insights faster
- Organise intelligence insights with simplicity and collaborate to improve resolution

To understand how Skurio can help protect what's important to your business and reduce your digital risk, please visit: **skurio.com.**

SKURIO

SKURIO LTD | ARTHUR HOUSE | 41 ARTHUR STREET | BELFAST | BT1 4GB

+44 28 9082 6226 info@skurio.com skurio.com