SKURIO

The essential guide to

Digital Risk Protection

skurio.com

If it feels like your business is playing a game of high-stakes catchup with cybercriminals - you are not alone

In the same way your company has digitally transformed, so have the hackers. They use the same advanced technologies that you do to make their business thrive — at the expense of yours.

My name is Justine Siebke, and I have spent the last three years researching how cybercriminals target your business before they attack.

Every organisation has a digital footprint: the apps you use, the digital assets you produce, your social media presence, your online storage, the partners who make up your digital supply chain and so on. Cybercriminals use this data to find easy targets, and then they strike.

There is, however, a light at the end of the tunnel.

This guide will show you how Digital Risk Protection can help you uncover your digital footprint and take steps to reduce your digital risk, sharing insights from information security professionals who are already doing it.

Contents

1 There is one universal truth: data breach is inevitable

How would you know if your business data is compromised?

Most businesses would be unaware: they usually only use security solutions that defend the network and data inside. Digital Risk Protection is different – it looks for breached data and threats to your organisation outside the firewall and beyond your network.

Digital Risk Protection focuses on protecting your data. Wherever it lives.

2 There are two kinds of data breaches

1. Human error

- Wrong email address
- Lost device
- Data theft

Your staff or your suppliers and partners can accidentally lose personal data (PII).

A misaddressed email or lost laptop incident can happen to any business. Information incorrectly distributed or lost is the biggest cause of PII data breaches in the UK.

2. Malicious attack

- Phishing
- Hacking
- Vulnerability exploit
- Ransomware
- Ex-employee

These can take many forms depending on the motivation for targeting your company.

Hackers may want to harm your reputation, disrupt operations, or profit financially from attacking your business. Bad actors could even include a former employee holding a grudge.

And, even if you have fantastic security and faultless processes, your business can still be at risk of attack through your supply chain.

3 Your data lives in three places

In the past, you knew precisely where your data was. Today, your business data is everywhere. For simplicity, this means three types of location.

1. Inside your network
- On-premise
- On private Cloud

Keeping control of on-premise data is straightforward enough.

No doubt, you already have systems in place to manage data security inside the firewall. Cloud security adds additional process and complexity.

2. Inside your digital supply chain
- Supply chain partners
- 3rd party apps

But, when data leaves the business, things start to get complicated.

Requiring suppliers to conform to standards is the first step; ongoing enforcement is more demanding. Not least because your partners and suppliers will also be reliant on their third-party suppliers, only increasing digital risk further.

3. Outside your business
- Devices
- Shadow IT
- Surface, Deep and Dark Web sites

And to top it all, data could be stored on devices or shared on emails using insecure networks.

All of this means that your data could end up in other locations, including the Dark Web, without your permission, knowledge, or protection.

How do you keep up?

4 You have four types of data to protect

Your business has digitally transformed to remain relevant and is data-driven in almost every aspect.

Your data is used to help define strategy, improve customer experience, accelerate research and development, drive recruitment and more. Loss or theft of data can impact your business significantly, especially if it falls into the hands of criminals or competitors. This data falls into four key types:

1. User credentials
- Login details and passwords for any systems used

2. IT infrastructure
- Software and infrastructure details that are useful to bad actors planning a cyberattack against you

3. Personal information
- Personal information (PII) about your staff, customers or other individuals that work with your organisation

4. Business-critical data
- Business-critical or commercially sensitive data that is necessary to provide services, run or organise your business

5 There are five compelling reasons to adopt Digital Risk Protection

Your business is facing increased digital risk on multiple fronts.

1. Increased cyber attacks
The threat landscape has increased in breadth and depth, with more attacks, more kinds of attacks, and more targeted attacks.

2. Digital transformation and cloud adoption
Digital transformation initiatives and the adoption of cloud services have spread data beyond the network and are providing bad actors with more opportunities to target your business.

3. Reliance on 3rd parties
This extended digital supply chain makes you reliant on multiple third parties to keep data safe.

4. Regulatory penalties
Data privacy regulations require increased compliance and diligence, with significantly heavier penalties.

5. Consumer trust
Consumers are increasingly aware of high-profile data breaches, making privacy and security key to maintaining customer trust and brand loyalty.

All this means that protecting your data within your network alone is no longer enough.

You need to protect your data. Wherever it lives.

6 There are six primary use cases for Digital Risk Protection

To illustrate how looking for compromised data and threats can keep your business safer, this guide explores the six primary use cases for Digital Risk Protection with real-life examples to answer these key questions:

What kind of information do cyber-criminals seek?

How could this data be used against you?

How could these threats increase your digital risk?

Monitoring for data breaches can help you protect your network from unauthorised access, avoid account takeovers and prevent successful phishing campaigns. Moreover, your team can add real business value by defending your brands and revenue when extending your existing security with Digital Risk Protection.

Protect your staff
Protect your infrastructure
Protect your customers
Protect your brand
Protect your revenue and margin
Protect your goods and services

6 There are six primary use cases for Digital Risk Protection

	 **Protect your staff.**	 **Protect your infrastructure.**	 **Protect your customers.**	 **Protect your brand.**	 **Protect your revenue and margin.**	 **Protect your goods and services.**
What we look for	• Data dumps • Credentials • PII / fullz • Credit cards • Mobile numbers • Domains • Email addresses	• IP addresses • Infrastructure details • Device details • Forum mentions • Port scans • 3rd party supplier mentions	• BreachMarker IDs • Customer data • Customer emails • 'Regex' pattern matches	• Brand names • URLs • Domain registrations	• Products • Loyalty card details • Pattern matches	• Product codes • Brands • Intellectual property
Threats we can prevent	• Phishing • Smishing • Account takeover • Identity theft	• Attack planning • Vulnerabilities • Supply chain attacks • Open port scan attacks	• Data sale or dump • Spam, scams and fraud • Phishing • Account takeover	• Typosquatting • Brand impersonation • Customer phishing • Activist targeting	• Discount abuse • Contract loopholes • Voucher abuse • Free downloads	• Intellectual property leak • Trademark infringement • Code theft • Counterfeit goods

Protect your staff

You store and process details about your staff on a surprising range of applications and sites, from HR and payroll to creativity and productivity tools.

But there could be many more services that fly under the radar.

Every time your staff use third party suppliers to sign-up for services and purchase goods, they spread data further, outside of your control.

Prevent account takeovers, phishing, and identity theft with data breach monitoring

3 things bad actors look for

- Credential breaches from apps that include plain text passwords
- Payment card details
- Personal information

3 ways they can use them against you

- Direct or brute force access to email systems, critical business applications or social media accounts
- Phishing and social engineering attacks Identity theft, fraud, and extortion attempts

3 ways this increases digital risk

- **Operational:** giving unauthorised access to commercial or back-office systems
- **Reputational:** spreading harmful or fake information about your brand
- **Resource:** doxing your senior execs or stealing trade secrets

The FBI says business email compromise cost US companies $1.8 billion in 2020. That's 64x the financial losses due to ransomware.

Own your playbook

- Set a clear policy for using third-party applications with corporate credentials
- Monitor for attack planning which targets members of staff
- Optimise breach response by integrating credential breach alerts with directory systems
- Send notifications to staff with compromised data and give guidance on steps they should take

4 easy ways to reduce risk

- Deploy multi-factor authentication to prevent external access to applications
- Use insights to educate users with poor password habits
- Promote awareness of phishing and social engineering methods
- Deploy a password manager tool for staff

Our customers agree...

"It's incredibly powerful when you see your information is on the Dark Web and you can see how easily it can be sold or shared."

IT Security Manager, International Consulting Firm

Close up

Staff credential breach

How your data is exposed

- **Insider threat:** credentials are leaked accidentally by your staff through misconfigured servers, an email sent to the wrong recipient or even deliberately.
- **Shared password:** internal leaks are more common when staff use shared credentials to access an application.
- **Third-party application breach:** even business-approved applications can suffer data breaches. Many major software companies, including LinkedIn, Adobe, and MyFitnessPal, have had credential breaches. If your staff have used corporate email addresses to sign up for these services, whether or not they are endorsed, you'll want to know that accounts are exposed.

What you can use to monitor for compromised credentials

- Email domain: **webnightsec.com**
- Staff list email addresses: **sales@webnightsec.com**
- Individual email addresses: **webadmin@webnightsec.com**

Monitoring results you might expect

- Posts that include matching email addresses
- Data dumps that include plain text passwords
- Forum posts offering exfiltrated data with sample details

Close up

Staff credential breach

How criminals can use this data to target your business

- **Spam:** fraudsters are always looking to obtain new datasets for spam campaigns to increase the chance of their success. Your staff could receive emails that include offensive content or bogus offers, for example.
- **Phishing campaigns:** even trained, experienced staff can fall for a convincing phishing attempt if it contains private details. These campaigns can result in your employees giving up further details (pharming) or clicking on a link that exposes them to malware.
- **Third-party system access:** automation makes it easy and quick to use credentials in brute force attacks. Unauthorised access could result in cyber criminals gaining access to multiple applications if an employee has reused passwords.
- **Account takeover:** hackers will attempt logins across multiple applications using exposed credentials. Vulnerable email, social media and retail website accounts are most likely to be exploited or taken over.
- **Extortion:** criminals blackmail your staff using sensitive information about them, content they post or their use of unapproved websites and apps.

Steps you can take that reduce risk

- Inform users to look out for phishing and extortion attacks
- Enforce password rotation
- Request takedown of post
- Implement password manager and multi-factor authentication to prevent future attacks
- Provide awareness training and use insights to educate users with poor password habits
- Deploy multi-factor authentication to stop account takeovers
- Update external service use policy

Close up

Staff credential breach

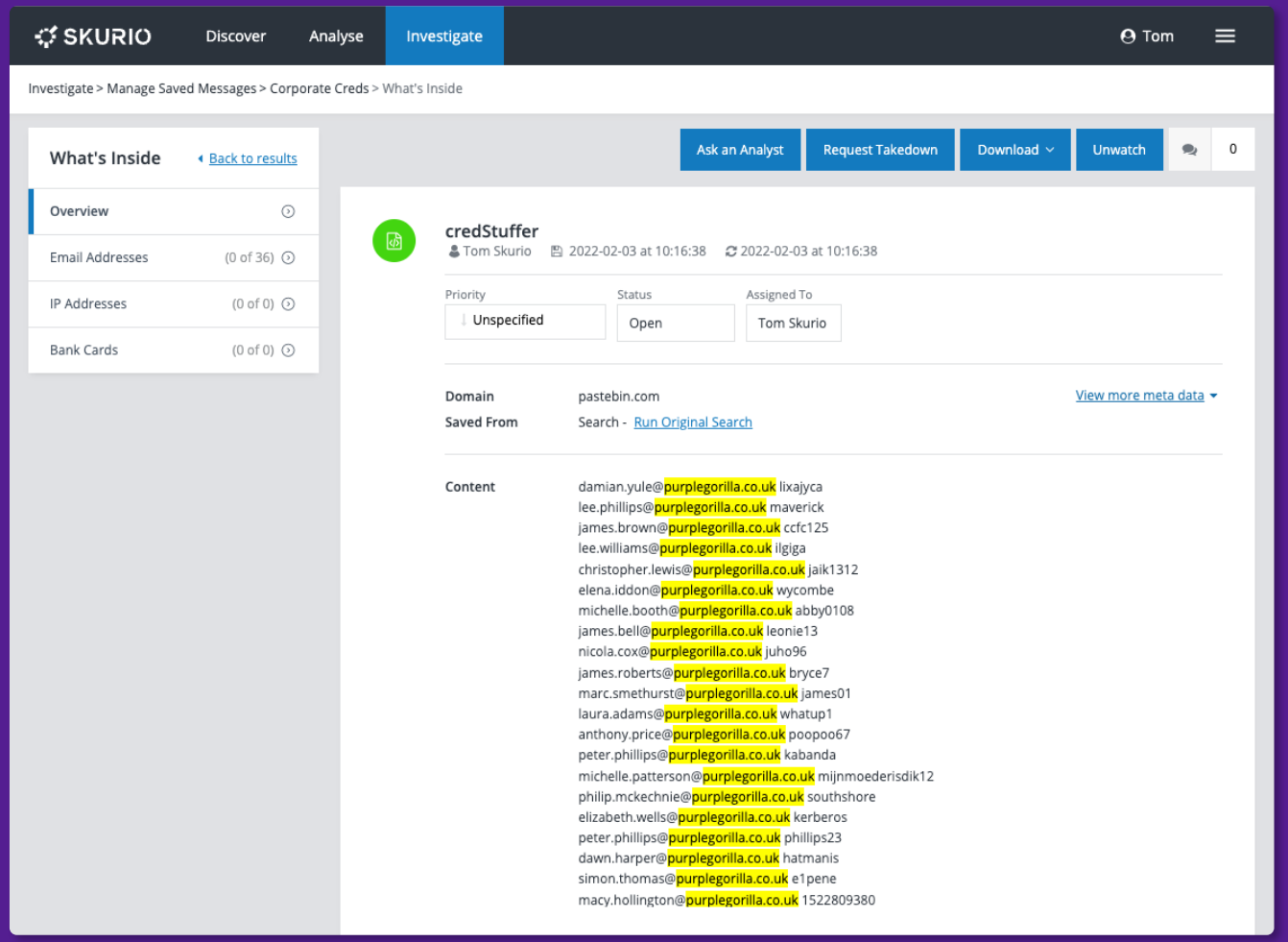
Pastebin credential dump

In this example, we searched for an email domain (purplegorilla.co.uk). A domain search is more efficient than maintaining a list of email addresses.

The results included this post on a Pastebin site containing 36 unique email addresses was found with plain text passwords.

The “What’s Inside” summary highlights any search term matches found in the result. Source information (metadata) helps with any incident investigation. Available metadata varies from site to site, here we can see the post link, author and language used.

Fraudsters could use the information in this post for phishing campaigns, social engineering, or to directly access applications that use the compromised credentials.



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

Extended use cases

	Leaked employee PII and card details Remote working has led to increased use of online services. Inevitably, your staff will use personal and payment card details with a wide array of suppliers. A breach from any one of these suppliers can lead to identity theft and fraud.	**VIP monitoring** Scammers could target individuals in your organisation for extortion, coercion, identity theft or harassment if their personal information is published online. Identifying compromised details for staff in high-ranking positions can help you take steps to prevent this kind of misuse.	**Leaked mobile numbers** Mobile phones improve access security for enterprise applications for authentication. If this information falls into the wrong hands, it can help hackers gain unauthorised access by cloning phones. Hackers can use mobile details to impersonate staff in social engineering attacks.
Details bad actors look for	• Personal details (PII) • Partial credit card details	• Personal details (PII) • Postcode • Social media handles	• Mobile phone numbers • IMEI & IMSI numbers
How they can be used	• Loan fraud • Payment fraud • Identity theft	• Email extortion or coercion • Online shaming or harassment • Physical attack • Social Engineering • Doxing	• Spoofing multi-factor authentication (MFA) • Social engineering • Physical staff tracking
How this increases digital risk	• Loss of creditworthiness • Loss of funds	• Insider threat, linked to extortion attempts • Staff absence or mental health issues resulting from cyber-bullying or blackmail	• Loss of operational systems • Exfiltration of data • Personal safety risk
Steps you can take	• Cancel payment cards • Report fraud • Improve procedures for online purchases	• Inform the target • Identify the source • Request a takedown • Inform authorities	• Use alternative MFA methods • Change mobile numbers • Improve awareness

Protect your infrastructure

Bad actors and criminals could be targeting your organisation already.

By collaborating and using techniques like port scans and reverse DNS lookups, they can get hold of valuable information about your network infrastructure, vulnerabilities, and the software you use.

It could be worse still if one of your team leaks sensitive information.

Stop the next attack on your infrastructure before it happens

3 things bad actors look for

- Domains, subdomains, and IP addresses
- Vulnerabilities in operating systems, hardware and software used
- Temporary storage and databases used for system testing

3 ways they can use them against you

- Denial of Service, either at a critical point (DoS) or distributed (DDoS)
- Vulnerability exploitation to deploy ransomware or malware
- Exfiltration of unprotected databases or digital assets

3 ways this increases digital risk

- **Reputational:** inability to provide service or capture new customers
- **Operational:** availability, confidentiality and integrity impacts on your systems
- **Revenue:** payment diversion, extortion or ransom could impact your bottom line

It's not all bad news

To plan attacks on your business, bad actors and criminals need information. To get this, they may access the Dark Web to buy, sell or share details about your infrastructure. They may discuss or collaborate on attack planning using hacktivist forums. And, when they do, they will often keyword terms specific to your business. Monitoring for these keywords can give an early warning of an imminent attack.

Automated early warning

- Automated Dark Web monitoring can check if your information is being discussed or circulated, and it works 24x7
- Instant alerts give you crucial hours, days or even months to implement mitigating steps

3 easy ways to reduce risk

- Close ports that are open unnecessarily
- Prioritise patch application and other measures to protect against exploitation of vulnerabilities discussed
- Deploy web application firewalls

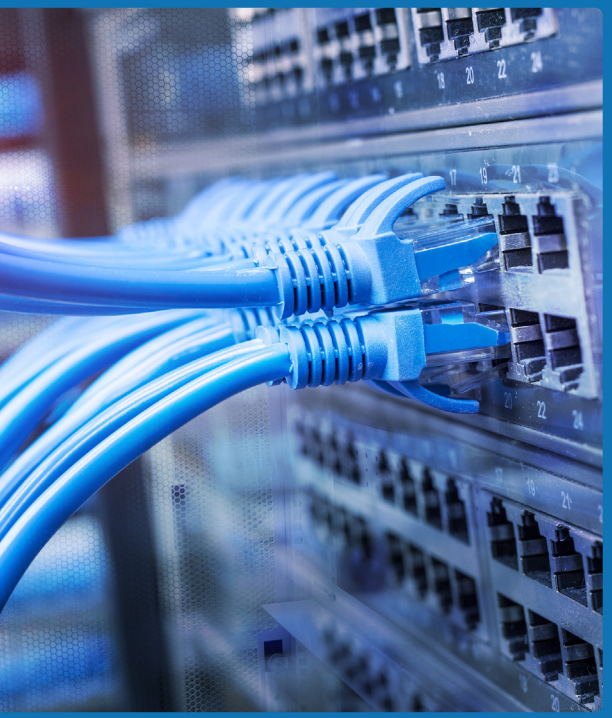
Our customers agree...

"If we didn't have this type of threat intelligence capability, we would be under attack before we even knew that we were under attack."

CISO, travel and tourism sector

Close up

Network information breach



How your data is exposed

- **Port scans:** Tools designed to help your security teams conduct penetration testing also provide hackers intelligence on exposed or poorly configured equipment and vulnerabilities. There is no specific law to prevent hackers from performing an 'aggressive port scan' on your network.
- **Domain whois:** Information about your domain registration, including expiration dates and similar available domains, can be discovered using a simple whois search.
- **Reverse lookup:** a reverse IP or name server (NS) lookup scan can provide hackers with details of all domains hosted on an IP address or name server. It could uncover unprotected contact details and allow hackers to monitor activity.
- **Insider threat:** A member of staff leaks important details about your infrastructure when asking for help with a technical issue on a support forum.

Details you can use to monitor for attack planning

- Individual IP address
- IP Address (range) search ("185.90.35.150")
- Domain and subdomain names
- Email addresses that have privileged system access

Monitoring results you might expect

- Published port scans or reconnaissance (recon) results
- Forum conversations that mention your company or staff
- Mentions of your company name in conjunction with known bad actors

Close up

Network information breach

How criminals can use this data to target your business

- **DoS/DDoS attacks:** denial or distributed denial of service attacks using recruitment of multiple parties.
- **Direct network attack**: attempted network penetration by exploiting a vulnerability.
- **Spearphishing:** phishing that targets an individual who has administration access to network infrastructure or network management tools.
- **Extortion:** fake ethical hackers target your company. These fraudsters will seek payment in exchange for giving you details of vulnerabilities you could have found yourself.
- **Typosquatting:** hackers use readily available details to register a typosquatting domain and impersonate your business.
- **Domain takeover:** without additional protection services, your domains are registered by activists if they lapse.

Steps you can take that reduce risk

- Address any vulnerabilities listed for software and equipment you use
- Deploy a web application firewall to reduce the impact of a DoS attack
- Inform staff of potential extortion attacks
- Request a takedown of posts containing sensitive details where possible
- Monitor for typosquatting domain registrations

Close up

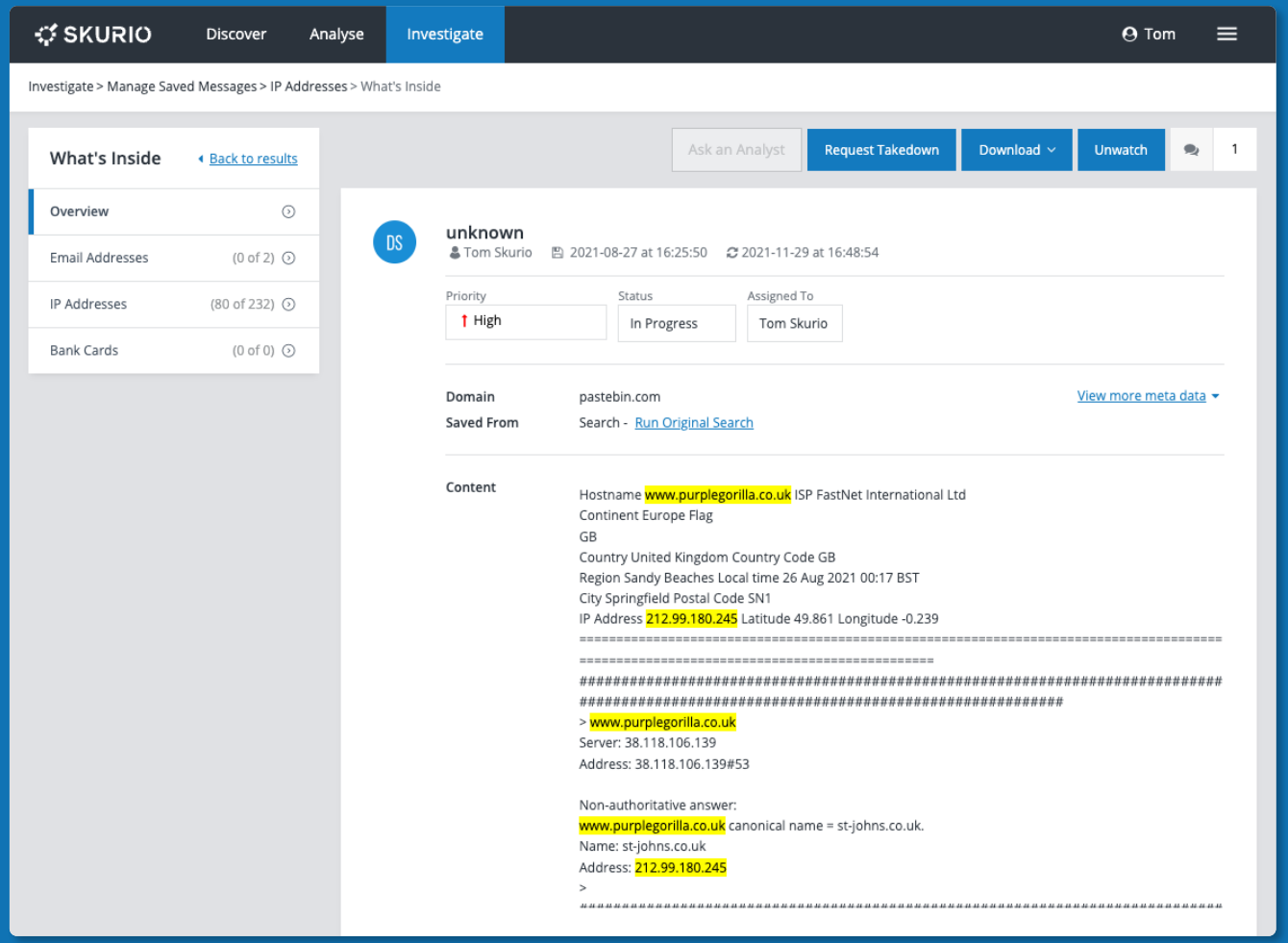
Network information breach

IP address and domain search

Widely available recon tools can capture infrastructure details. These tools can highlight vulnerabilities, including open ports or unpatched servers.

If they are shared on dumpsites, as this example shows, or discussed in forums, your organisation could become a target of hackers.

Without monitoring or conducting manual searches every day, this exposure can go unnoticed. A simple takedown request can get the content taken down and the risk reduced.



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

Extended use cases

	Indicator of attack planning Known threat actors discuss your company on forums in conjunction with attack methods, indicating that a cyber-attack is imminent or likely.	Ransomware If a new vulnerability affects your infrastructure, your business could become a target for ransomware gangs. So, scanning for mentions of your business in discussions about vulnerabilities is vital. Posting exfiltrated data regardless of ransomware payment is a recent trend with ransomware gangs. Any company experiencing a ransomware attack should monitor for leaked data.	Supply chain compromise Swift detection of data breaches or vulnerabilities in your supply chain is key to preventing follow-on incidents like ransomware attacks and reducing financial exposure. Monitoring for supplier information can provide an early indicator of supply chain vulnerabilities, attack planning or attacks in progress.
Details bad actors look for	• Brand or company name mentions alongside potential threat actors or attack methods	• Newly discovered vulnerabilities • Published recon details • Credential breaches from your supply chain partners	• Newly discovered vulnerabilities • Published recon details • Credential breaches from your supply chain partners
How they can be used	• To recruit additional individuals to assist with the attack • Claiming responsibility for an attack • Discussing the best way to target your business	• Direct cyber-attacks on your partners that result in leaks of your data or intelligence on your operations • Exploiting access to your infrastructure that you have granted to your partners	• Direct cyber-attacks on your partners that result in leaks of your data or intelligence on your operations • Exploiting access to your infrastructure that you have granted to your partners
How this increases digital risk	• Loss of operational systems • Loss of customer and partner trust • Loss of business/income	• Exfiltration of customer data • Extortion • Supply chain compromise	• Exfiltration of customer data • Extortion • Supply chain compromise
Steps you can take	• Address outstanding vulnerabilities • Add additional protection to critical assets	• Add BreachMarker IDs to identify customer data leaks from partners • Notify partners of potential threats so they can act • Monitor for exfiltrated data dumps from supply-chain partners that include your content	• Add BreachMarker IDs to identify customer data leaks from partners • Notify partners of potential threats so they can act • Monitor for exfiltrated data dumps from supply-chain partners that include your content

Protect your customers

Customer trust is a bedrock for loyalty and business growth.

One recent IBM survey reported an average 3.9% higher churn rate for businesses that had suffered a customer data breach.

According to RSA, 35% of consumers use false details when creating accounts - because they don't trust brands to keep their data safe.

Digital trust is the new frontier — give customers confidence in your services

3 things bad actors look for

- Unprotected databases exposed on Cloud infrastructure
- Opportunities to inject code into web plugins like payment or chat applications
- Staff or supply chain partners who are willing to leak or sell customer details

3 ways they can use them against you

- Customer data, including PII, is shared or sold via the Dark Web
- Fraudsters use email lists for spam, phishing, or payment diversion
- Skimming customer payment details by form-jacking

3 ways this increases digital risk

- **Reputational:** customers lose trust and turn to competitors
- **Operational:** downtime of service, loss of access to critical data
- **Financial:** loss of revenue, ransom payments, compensation, and regulatory fines

Protect your data. Wherever it lives.

Customer data doesn't just live inside your network. Cloud storage and apps, 3rd party services and partners can still lose data, no matter how good your network defences are. Minimise the potential fallout and damage of data breaches by watermarking your data and continuously monitoring for leaks.

Best-practice is key

- Data privacy is important to your customers. Have a clear policy and stick to it
- Make sure your partners take data security seriously too
- Use Digital Risk Protection techniques to protect data beyond your network

3 easy ways to reduce risk

- Watermark your data with unique synthetic identities to spot leaks
- Deploy multi-factor authentication for customer access to your services
- Monitor for your customer data on the surface, deep and Dark Web and report breaches without delay

Our customers agree...

"As a leader in our industry, maintaining our brand reputation and the trust of our customers is vital. Skurio provides us peace of mind with minimal day-to-day effort."

Security Manager, Industrial Manufacturing

Close up

Customer data breach

How your data is exposed

- **Insider threat:** sending customer details to the wrong email address or storing customer data on an unprotected device that is lost or stolen are among the most frequent causes of a data breach.
- **Shared password:** using a shared login for an app is sometimes unavoidable. Criminals can gain access to these applications and the data they store if staff use poor passwords or share credentials in an insecure way. This kind of breach is challenging to detect using traditional security tools.
- **Supply chain breach:** customer data leaked by suppliers is your responsibility too. An upfront security questionnaire provides no guarantee of breach avoidance.

Details you can use to monitor for customer data breaches

- Customer email list
- Hashed customer email addresses
- Synthetic identities inserted into your customer datasets
- Your company name/domain

Monitoring results you might expect

- A new data dump includes customer credentials that match your data
- A post that mentions your company or web domain contains customer email addresses and password combinations
- A compilation breach incorporates your customer data

Close up

Customer data breach

How hackers use data to target your customers or business

- **Phishing:** campaigns that impersonate your brand can expose your customers to malware, social engineering attacks or pharming (harvesting sensitive details).
- **Account takeover:** data breaches that contain password information can leave your customer accounts vulnerable to takeover.
- **Fraud:** Customers could be offered counterfeit or stolen goods by fraudsters impersonating your business.
- **Payment diversion:** Customers could be sent payment requests that appear to come from your business.

Steps you can take that reduce risk

- Identify the scope and impact of the breach on your organisation
- Maintain a clear communications policy so that customers know where to get information if an incident is ongoing
- Inform customers to anticipate phishing attempts and force password change
- Inform the responsible regulatory authority (e.g., ICO) to minimise GDPR fine - all customer data breaches are reportable
- Watermark data to establish the origin of any breach
- Where possible, issue a post takedown request to remove the shared data
- Identify the breach source and mitigate against future risk

Close up

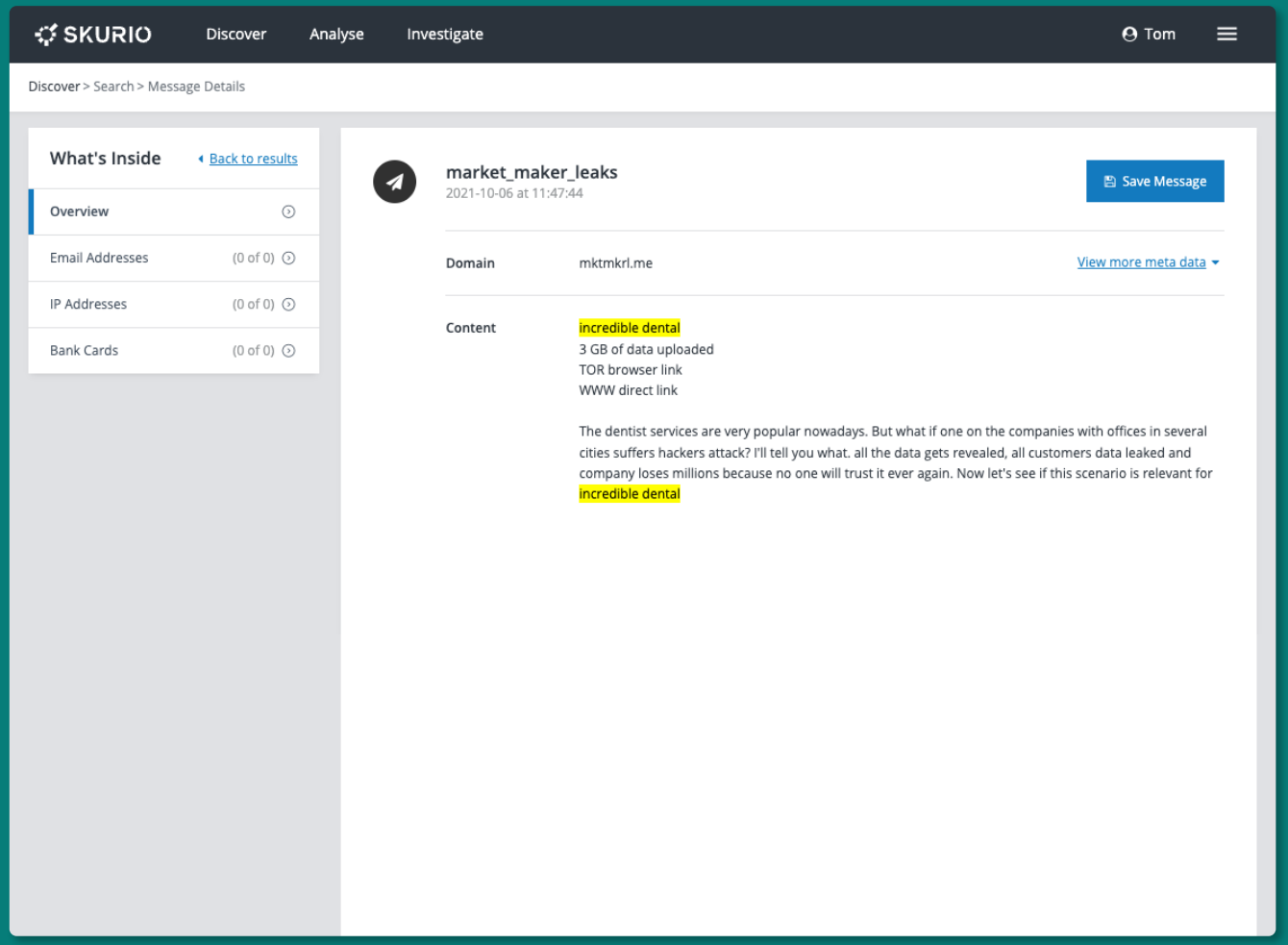
Customer data breach

Promoted Dark Web link to customer data

New data breaches that come with a clear provenance are very valuable.

Selling or sharing them on Dark Web forums and marketplaces helps them remain anonymous but restricts their audience. By scanning messaging forums, you can detect attempts to promote the data.

This example shows a Telegram post that advertises a link to the Dark Web.



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

Extended use cases

	Spam lists Many believe a leak of customer email addresses without passwords or PII is a relatively minor incident. However, fraudsters can use these lists in phishing emails that put your customers at risk of malware or pharming campaigns. Hackers can also combine email lists with common passwords in dictionary attacks to takeover email or application accounts.	Dark Web data sale Fresh data dumps are extremely valuable to cyber-criminals. Data will be offered for sale via Dark Web markets to maximise the value, using a small sample of data. If data dumps contain payment or personal information, fraudsters can use these details in fraud, phishing and identity theft.	Account takeover Swift detection of customer data breaches is key to preventing follow-on attacks and reducing financial exposure. If criminals get hold of customer account credentials, they could use unprotected accounts to order goods and services or cash in by selling them.
Details bad actors look for	• Customer data for sale • Shared data dumps	• Customer data for sale • Shared data dumps	• Accounts offered for sale on forums or marketplaces • Credential data dumps • Exfiltrated data from ransomware attacks
How they can be used	• Monetised through resale on the Dark Web • Phishing / Smishing • Social engineering	• Monetised through resale on the Dark Web • Phishing / Smishing • Social engineering	• Facility takeover • Theft of goods • Fraud
How this increases digital risk	• Loss of trust • Customer churn • Loss of revenue • Regulatory fine	• Loss of trust • Customer churn • Loss of revenue • Regulatory fine	• Loss of revenue • Customer churn • Regulatory fine • Theft
Steps you can take	• Monitor for customer data using secure DRP • Identify and address the source of the leak • Notify customers and enforce a password reset	• Monitor for customer data using secure DRP • Identify and address the source of the leak • Notify customers and enforce a password reset	• Add BreachMarker IDs to identify compromised customer data • Monitor for customer data using secure DRP • Notify customers and enforce a password reset

Protect your brand

Your digital brand is continuously at risk of attack.

Misinformation and complaints from customers, trolls, activists or competitors can damage your reputation. But your company and brand could be targeted by fraudsters too.

According to fraud experts Cifas, business impersonation grew 23% in 2020. Scammers use typosquatting domains to impersonate your business because it increases the chances of a successful phishing campaign.

Complaints from upset customers who have lost money or had sensitive details harvested could be the first you hear about it.

Stop fraudsters from impersonating your business

3 things bad actors look for

- Available domains that could fool customers in phishing or fraud campaigns
- Document templates for counterfeit invoices or fake receipt generators
- News stories they can hijack to execute scams

3 ways they can use them against you

- Phishing, smishing or online campaigns to drive traffic to sites that spread malware harvest sensitive details (pharming)
- Sale of stolen or counterfeit goods that undermine your business
- Payment diversion scams using fake invoices

3 ways this increases digital risk

- **Reputational:** customers scammed by someone impersonating your business stop using services
- **Revenue:** sales of fake or stolen goods may impact your sales
- **Revenue:** domain takedowns can involve lengthy and costly legal battles

It's not all bad news

If a fake website contains your trademarked content or enables illegal activity, you are within your rights to request it to be taken down. Fast detection of newly registered and suspicious domains improves the chances of a successful takedown to escape damage to your reputation and bottom line.

Automated early warning

- Get instant alerts when a suspicious domain is registered and help with takedowns
- Detect fake documents that fraudsters can use to trick customers
- Mentions of your company or brands in hacktivist discussions

3 easy ways to reduce risk

- Trademark brands and products to protect your online presence
- Register key top-level domains to prevent scammers from registering them
- Implement easy ways for your customers to report and learn about scams

Our customers agree...

"It doesn't have to be complicated, and that's what we love about the platform. It's easy to use and has great functionality"

Amber Burridge, Head of Fraud Intelligence, Cifas

Close up

Typosquatting and domain impersonation campaign

How your domains are compromised

- **Lapsed domains:** existing domains that expire are re-registered by fraudsters.
- **Unused TLD domains:** unregistered domains you don't use for other Top-Level Domains (TLDs), for example, country domains ".co.de" or category domains ".store" or ".support" – Wikipedia maintains a complete list.
- **Typosquatting variations:** domain variations for your brands or products they can use to fool customers or capture traffic from users who have mistyped your site address.
- **Cybersquatting domains:** fraudsters register unused domains for products, services or brands.

Details you can use to monitor for suspicious domains

- Domains in use
- Brand names
- Product/service names

Monitoring results you can expect to find

- Historically registered domains
- Newly registered domains
- Change of use/change of ownership

Close up

Typosquatting and domain impersonation campaign

How data can be used to target your customers or business

- **Phishing:** phishing campaigns that impersonate your brand can expose your customers to malware or social engineering attacks.
- **Pharming:** scammers use a fake domain for pharming – gathering sensitive information that can leave your customer accounts vulnerable to takeover.
- **Fraud:** criminals will use domains to offer counterfeit and stolen goods or execute other scams.
- **Profiteering:** a URL that impersonates your business is used to capture and redirect traffic to your site but monetises it through advertising.

Steps you can take that reduce risk

- Register any important TLDs
- Trademark your brands and logos etc.
- Monitor for newly registered domains that include your brand, product, or service names.
- Monitor for changes in use – e.g., added email service or change of ownership
- Add suspicious domains to reporting services like Google safe browsing
- Get the site removed using a takedown service
- Use DNS filtering to prevent staff from visiting suspicious domains

Close up

Typosquatting and domain impersonation campaign

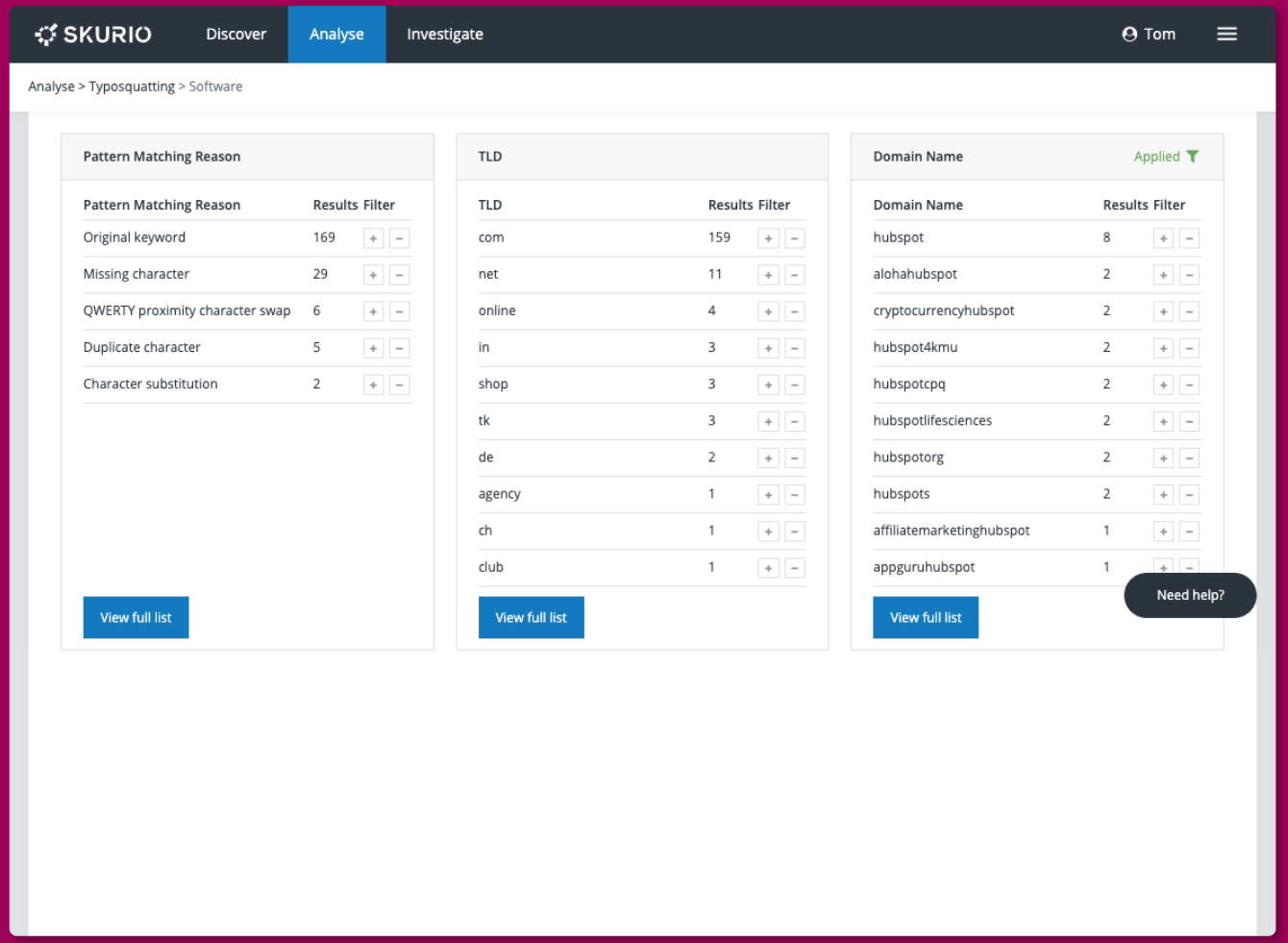
Spoofing the domain of a popular business software app

There are many ways to generate a typosquatting URL– this example for a popular marketing tool shows four methods.

Most malicious domains, however, use a 'long tail' version of the keyword term. 'appguruhubspot' is a great example – the site is probably legitimate but worth checking, in case it contains poor quality content that could damage the brand.

Registrations for new TLDs that are identical to the brand name but use a new TLD - there are eight in this example - are suspicious if not registered by your organisation.

Always use a specialist takedown service if you believe a domain is spreading malware or involved in illegal activity.



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

Extended use cases

	Customer phishing Criminals use branded documents and templates to trick customers into paying fake invoices, changing their direct debit set up or providing other sensitive information.	**Brand impersonation** Bad actors use fake profiles to impersonate your company or employees. These campaigns can scam customers or spread harmful content about your brands.	**Hacktivist targeting** Your business can be the target of misinformation, defamation, or disruption campaigns if it operates in a controversial sector or has policies that attract the interest of hacktivist groups.
Details bad actors look for	• Company documents examples • Invoice templates shared or sold	• Social media accounts that impersonate your company or VIPs • Posts on sites or messaging forums that pretend to come from your business	• Evidence of business activity that conflicts with their beliefs • Opportunities to get involved in targeted campaigns to improve their reputation in the hacker community
How they can be used	• Payment diversion scams using fake invoices	• Spread misinformation • Harm the reputation of individuals • Scam your customers	• To recruit additional individuals to help with campaigns • Claiming responsibility for an attack • To discuss the best way to target your business
How this increases digital risk	• Loss of trust • Customer churn • Loss of revenue • Regulatory fine	• Loss of trust • Customer churn • Reputation damage	• Reputational damage • Loss of trust
Steps you can take	• Request takedown of posts containing branded documents • Inform and warn customers • Report fraud to relevant authorities	• Improve ways for your customers to report scams • Request a takedown of accounts or posts • Report illegal content to relevant authorities	• Monitor for supplier/product name mentions alongside potential threat actors or attack methods • Request takedown of defamatory or inaccurate content • Report illegal activities to the relevant authorities

Protect your revenue and margin

Everyone loves a bargain.

In one survey, 80% of shoppers said a promotional discount would encourage them to make a first-time purchase. They also encourage repeat business for 91% of customers.

If scammers or genuine customers abuse these discounts, they can erode your margin and hurt your bottom line.

Your business works hard to deliver your products and services, don't let customers get them for free

3 things bad actors look for

- Discount codes
- Service hacks and workarounds
- Staff willing to share exploitable information

3 ways they can use them against you

- Sharing codes online
- Counterfeiting physical vouchers
- Sharing loopholes with competitors

3 ways this increases digital risk

- **Operational:** reduced ability to remain competitive
- **Financial:** reduced margin on service or product sales
- **Regulatory:** potential fines under consumer protection laws

Look for loopholes outside your network

Monitoring for contract and discount abuse methods can help you crack down on unnecessary losses and give your teams time and resources to get special offers into the hands of the customers you want to attract, with watertight contract terms.

Go beyond credential monitoring

- Use Digital Risk Protection to monitor for sharing and misuse of discounts and promotions
- Monitor active threat actors who share discount details or service hacks

4 easy ways to reduce risk

- Use one-time, user-specific discounts and promotions
- Use unique codes to track public sharing
- Consider requesting a takedown of publicly posted data
- Identify source to prevent further loss

Our customers agree...

"It's been an enormous success story. We've been able to open up a whole avenue of intelligence that people were not looking at before."

Finance Operations Manager, communications sector

Close up

Discount abuse

How your discount schemes are compromised

- **Vigilant consumers:** if it is possible to abuse your discount scheme, it won't take your customers long to find out
- **Insider threat:** opportunistic staff use insider knowledge to develop a lucrative side-hustle
- **Accidental loss:** a promotional email campaign sent to the wrong group of customers

Details you can use to monitor for threats

- Company name, brands, and product names
- Business terms used to describe your promotions
- Promotion codes

Monitoring results you can expect to find

- Mentions of your products and services
- Publication of discount codes
- Posts describing how to get your products and services cheaper or for free

How scammers target your business

- **Disclosure:** sharing discount codes on specialist forums is commonplace
- **Hacktivism:** widespread sharing of codes or service hacks from campaigners who want to disrupt your business
- **Scams:** scammers lure customers into giving sensitive information or expose them to malware using fake discount codes

Steps you can take that reduce risk

- Use unique codes to improve tracking
- Request a takedown of information from the site
- Identify the source of the breach and mitigate against future risk

Close up

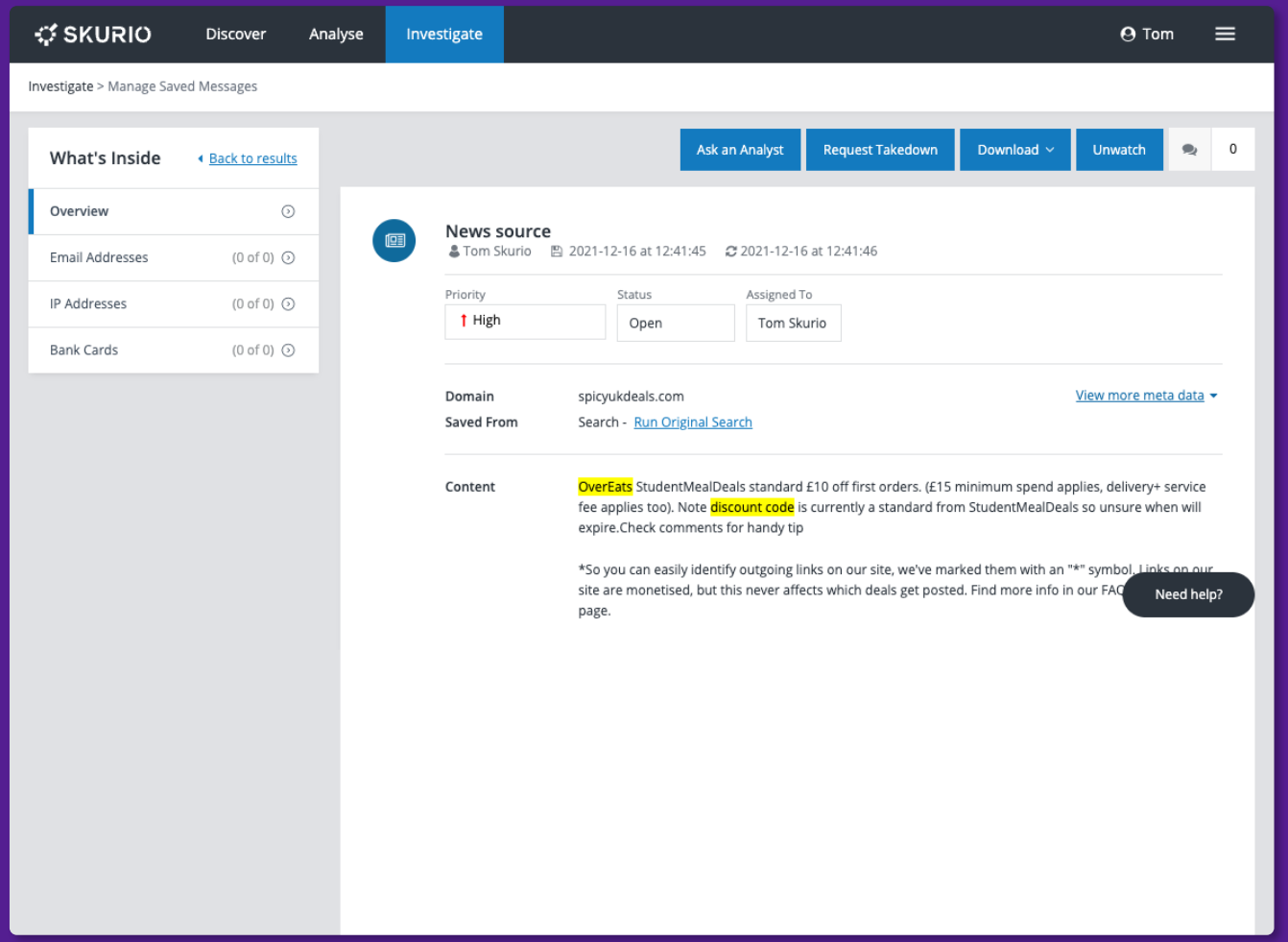
Discount abuse

Public sharing of a student discount code

Discount forums frequently share codes created for a specific consumer group.

This example shows a student discount for a popular food delivery service. An affiliate partner promoted the offer on its website, and this link is shared publicly and available to any customer using this tip.

Discount abuse is widespread but often goes undetected. Monitoring for it with a Digital Risk Protection solution is straightforward and makes good business sense.



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

Extended use cases

	Contract loopholes There is a popular misconception that consumers never read the small print. But a small minority do. And, if they find a loophole that allows them to cancel a service without ever paying or avoiding penalties – your business could be at risk of widespread exploitation. Cyber create multiple fake accounts to earn bonuses using automation tools. Once the account setup is complete, they can cash out by selling them.	**Voucher/receipt abuse** A promotion that's great for customers can be great for criminals too. Document templates allow consumers to print vouchers with valid codes for use in-store or return stolen goods with fake receipts.	**Free downloads** Digital products are attractive to criminals and hackers because they can sell them on marketplaces without physical logistics in place. Alternatively, activists who believe copyright is not morally justified could share your content and products for free.
Details bad actors look for	• Sign up incentives for services that do not require a purchase • Codes shared or sold for promotions not wanted or needed by the original recipient • Mistakes that result in under-priced goods and services	• Examples of vouchers they can use in template generation • Shared photos of receipts that show your proprietary formats	• Unprotected software products or code • Videos or music offered for download • Advertisements or listings of free digital publications or books
How they can be used	• Social sharing • Sharing of sensitive information with competitors • Monetised through Dark Web sales	• Monetised through Dark Web sales • Handling stolen goods • Receipt-as-a-service	• Shared for free via forums or torrents • Monetised through Dark Web sales
How this increases digital risk	• Loss of revenue • Customer churn • Competitive disadvantage	• Loss of revenue • Competitive disadvantage	• Loss of revenue • Copyright protection litigation
Steps you can take	• Monitor for brand name mentions in conjunction with contract loophole keywords • Use DRP to scan for cash-out guides that cite your brands • Update terms and conditions • Request takedown of shared information	• Use DRP to monitor for keywords used by your promotion • Document templates offered for receipt or voucher printing • Identify and address the source of the leak • Request takedown of shared information • Inform relevant authorities of illegal activity	• Safeguard content with copyright protection • Request a takedown of the post • Inform the relevant authorities of illegal activity • Identify and address the source of the leak • Watermark products and code then monitor using DRP

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

Close up

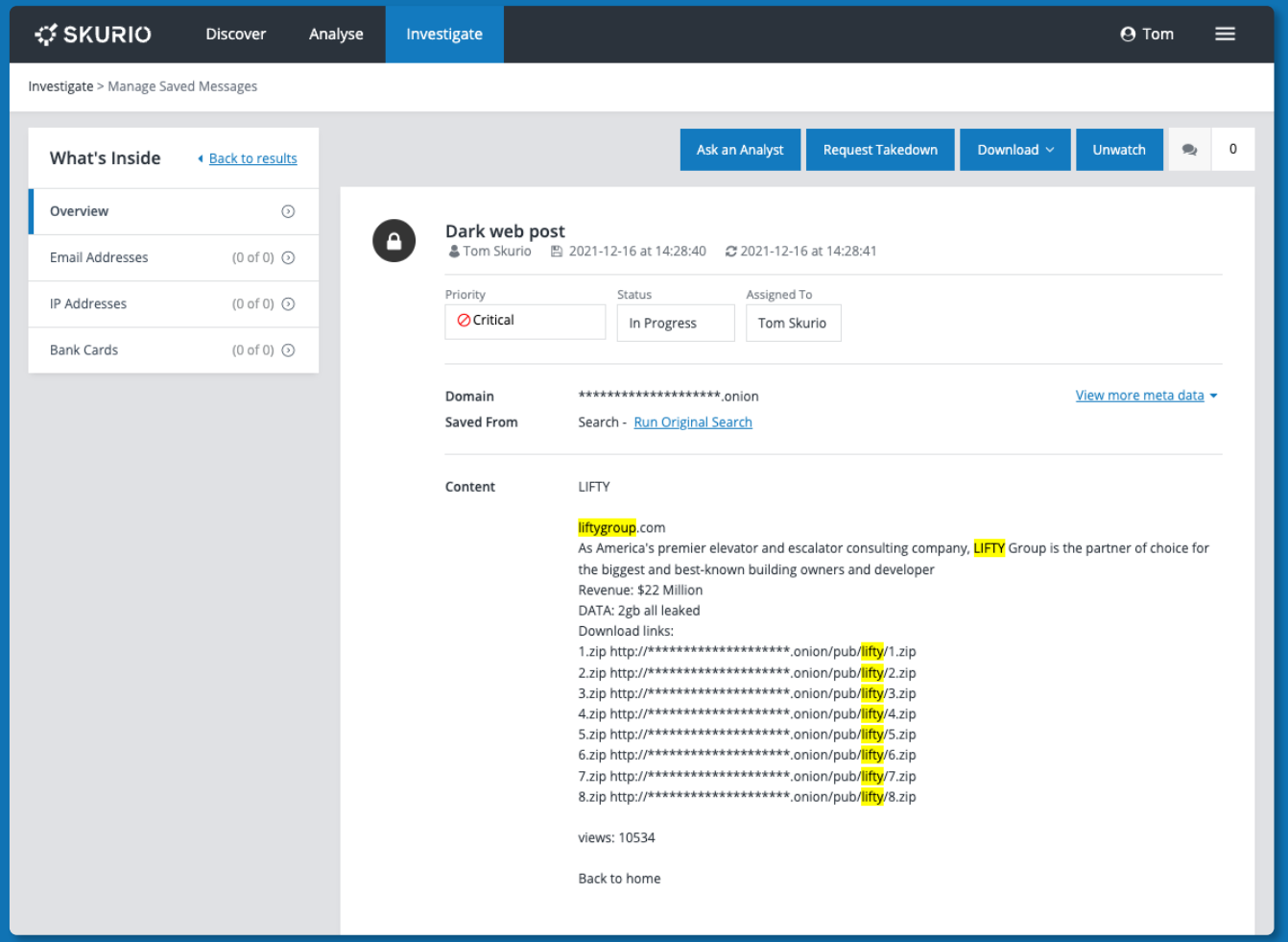
Critical business data breach

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.



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**