SKURIO

The essential guide to

Digital Risk Protection

Protecting your customers

skurio.com

SKURIO

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.

SKURIO

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

SKURIO

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

SKURIO

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

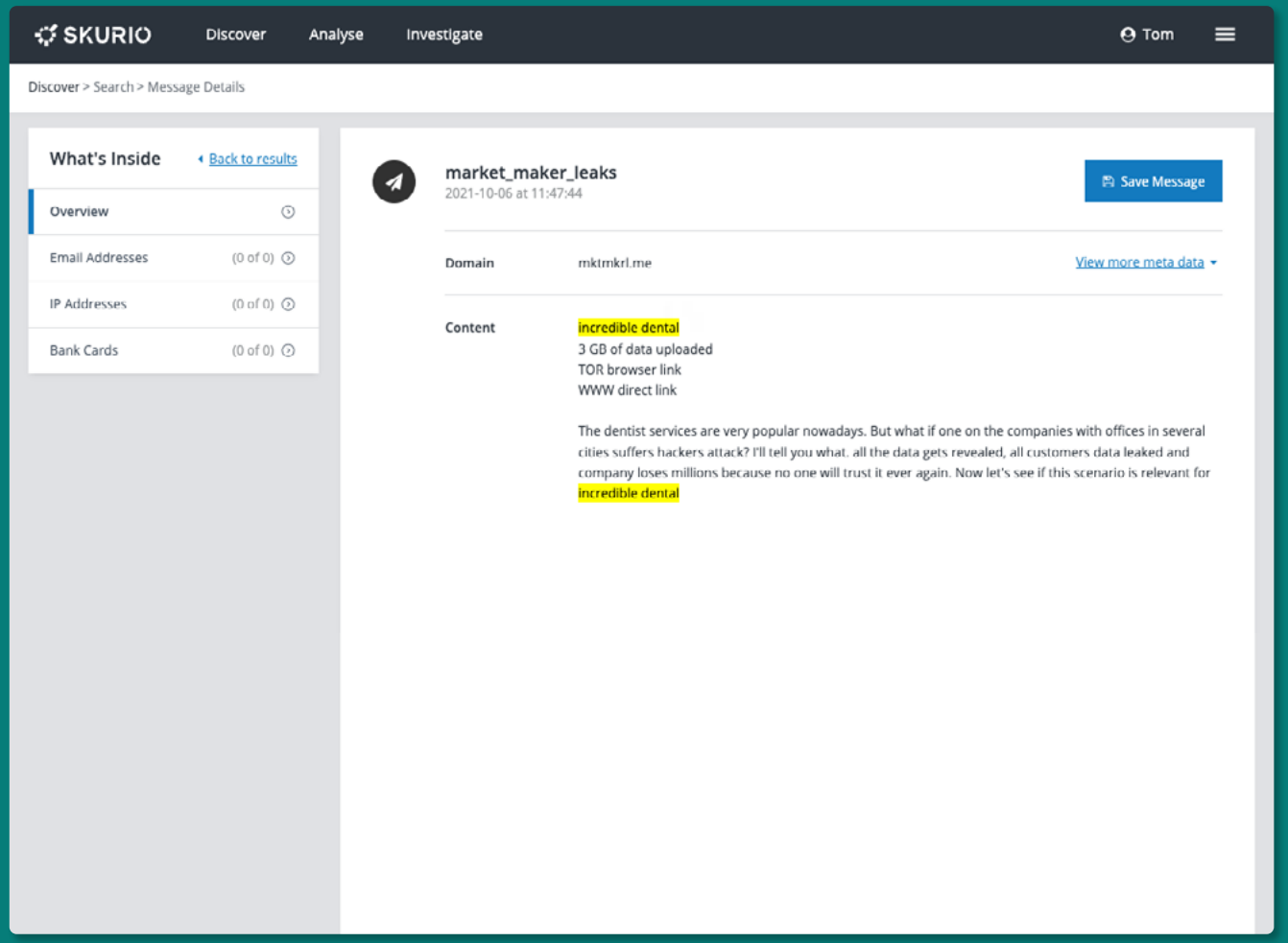
Customer data breach

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	Dark Web data sale	Account takeover
	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.	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.	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

SKURIO

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
OPEN