RED SIFT

eBook

6 STEPS TO BECOMING DIGITALLY RESILIENT IN TIME FOR DORA

Contents

Introduction

The Digital Operational Resilience Act (DORA) is set to transform how financial firms in the EU (and any global financial firms that want access to the EU market) protect themselves, their consumers, and investors from cyber risks. In essence, the legislation requires these businesses to recognize and mitigate any reasonably identifiable circumstances that could lead to an event that could compromise the digital operational resilience of the firm and by extension protect the broader financial sector.

DORA's impact won't just be contained to EU financial firms, and the comprehensive legislation will have wide-reaching global significance primarily for two reasons. The first is that it impacts **any** financial or third-party software organization that needs to access the EU market, in this case making it applicable worldwide. The second is that it sets a benchmark for organizations of all sizes in all sectors globally to look to improve their digital operational resilience. Ultimately, any organization concerned by cyber threats would do well to use DORA as a guidebook to improve digital resilience. DORA is expected to arrive this year (2022) and be fully enforced by 2024, it's crucial all impacted businesses start preparing now.

DORA is a lengthy piece of legislation, and it would be impossible to address every provision that businesses need to prepare for in this eBook. So instead, we'll address what we believe are the top 6 provisions that are reasonably achievable in a short time frame. As with preparing for any new legislation, it's worth involving your lawyers. However, we hope this eBook is a useful starting point, particularly in mitigating threats as they relate to email and domain security.

This initiative has been led by Red Sift's Head of Cyber Governance and DORA subject matter expert Rois Ni Thuama LLB LLM PhD. Rois is Adjunct Professor at Ireland's leading technical university, Munster Technical University (MTU) and is recognized as an expert in the field of Cyber Governance, risk and compliance. She is frequently invited to speak at public events. She has spoken at the NYPD's Cyber Crime and Counter Terrorism Symposium, the International Fraud Prevention Conference, e-Crimes, and has spoken on panels alongside serving members of the Federal Bureau of Investigations (FBI), the US Department of Defense and the US Department of Justice. She is part of the keynote panel in the upcoming InfoSec in her role as ambassador with the Global Cyber Alliance. This summer Dr. Ni Thuama joins the team driven by the NATO initiative tasked with revising the cybersecurity curriculum for member countries.

If you're reading this, there's a good chance you have an understanding of what DORA is and why it's time to get started with implementing it. If not, then download our whitepaper here: DORA: Better, Faster, Stronger: Your Guide to the Digital Operational Resilience Act

What is DORA?

The Digital Operational Resilience Act (DORA) is European legislation that requires any financial organization in the European Union (EU) or accessing the EU market to have safeguards in place to mitigate cyber threats. Firms will be required to ensure they can withstand all types of ICT-related disruptions and threats.

Who DORA affects:

DORA applies to any EU business that manages, transfers, holds, insures, invests, creates, protects, raises, or grades money, plus third-party software providers.

- Banks
- Auditors and Audit Firms
- Investment Firms
- Management Firms
- Credit Institutions
- Insurance & Reinsurance Firms
- Brokers
- Credit Rating Agencies
- Crowdfunding Services
- Trading Venues
- Trade Repositories
- Crypto-Asset Providers
- ICT Vendors
- Provides Digital and Data Services
- Cloud Computing
- Software
- Data Analytics
- Data Centres

DORA doesn't just impact EU headquartered firms, it applies to any financial firm that has offices in the EU, or wants access to the market.

DORA will make businesses Better, Faster, and Stronger, and some of the benefits include:

- Stronger business resilience
- Better and faster decision making
- Protection from opportunist criminals
- Clear and comprehensive guidelines
- More robust supply chains
- Defensibility in the event of an attack
- Smoother exit strategies

Who's responsible?

The final responsibility to ensure that measures, policies, tools, and protocols are enacted to mitigate cyber **threats** sits with the management body. Failure to do so could result in:

- ⚠ Reputational damage
- ⚠ Shareholder litigation
- ⚠ Regulatory fines
- ⚠ Criminal sanctions

Step 1. Educate your board

What DORA says:

> *Members of the management body shall, on a regular basis, follow specific training to gain and keep up to date* ***sufficient knowledge and skills*** *to understand and assess ICT risks and their impact on the operations of the financial entity.*
>
> DIGITAL OPERATIONAL RESILIENCE ACT (DORA), ARTICLE 4 (4)

What we say:

While directors have almost always been legally obligated to exercise care, skill, and diligence[1], this hasn't always been implemented with respect to cyber threats, risk, and cybersecurity. Instead, the view was that it belonged not to the board as a whole but to a subset of the board. DORA displaces that misconception and unequivocally holds the entire management body responsible.

Because management now bears the full and 'final responsibility for managing' the firm's cybersecurity risks, they must come to terms with developing a broader understanding based on practical and proven cybersecurity frameworks. They must deepen their understanding with clear insights from experts. Relying on experts is essential as any decisions made at this level could be subject to review. Ultimately, the courts expect business decisions to be:

- Informed
- Based on *expert* advice
- To the benefit of the company as a whole.

> *In recent years, cyber threats, associated risk, and cybersecurity are now being considered by C-Suite as part of the overriding corporate strategy. This sees a shift from value generation only to value generation alongside value preservation in defense of the firm. The implications for businesses and boards who fail to take reasonable care are criminal penalties, fines, shareholder derivative action, and reputational damage.*

Rois Ni Thuama, PhD
HEAD OF CYBER GOVERNANCE
RED SIFT

Step 2. Implement the right systems, protocols, and tools

What DORA says:

> *Where financial entities use internationally recognized technical standards and industry-leading practices on information security.*
>
> DIGITAL OPERATIONAL RESILIENCE ACT (DORA), ARTICLE 6 (2)

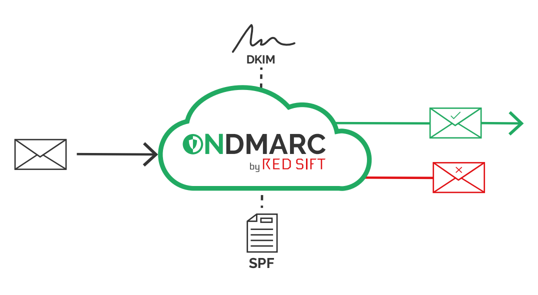
What we say:

At Red Sift, everything we do is led by globally recognized standards and informed by trusted, independent experts. Now, DORA means affected financial firms and third-party software providers must ensure they do the same. While this applies to mitigating risk in all areas, email and domain security is no exception, given that email is a top vector for cyberattacks[2].

Making DMARC reliable and easy with the Red Sift Platform

This is where DMARC comes in, as highlighted by the National Institute of Standards and Technology (NIST) Trustworthy Email (special publication)[3]. Ultimately, firms can be confident that by implementing DMARC correctly, they're complying with DORA's guidance on mitigating risks relating to email and domain security.

What is DMARC?



DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an outbound email security protocol that - when implemented at the strongest policy of p=reject - protects domains against exact impersonation i.e. when a bad actor impersonates an organization's domain to send phishing emails to its employees, customers, and supply chain. It works using existing protocols SPF and DKIM.

DMARC is globally-recognized, robust, and widely acknowledged to be the fundamental layer for outbound email security and defense against phishing and BEC. It's recommended and/or mandated by:

National Institute of Standards and Technology (NIST)

The UK's National Cyber Security Centre (NCSC)

The Center for Internet Security

The US Department of Defense (Cybersecurity Maturity Model Certification - CMMC)

The US Federal Government Pursuant to the Binding Operational Directive 18-01

The British Government in the Minimum Cyber Security Standards

What NIST says:

> *Technologies recommended in support of core Simple Mail Transfer Protocol (SMTP) and the Domain Name System (DNS) include mechanisms for authenticating a sending domain: Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).*
>
> **NIST TRUSTWORTHY EMAIL SPECIAL PUBLICATION 800-177**

What DORA says:

> *Inspired by relevant international, national and industry-set standards, guidelines, recommendations or approaches towards the management of cyber risk.*
>
> **(SEE DORA FOOTNOTE 37, RE: NIST CYBER SECURITY FRAMEWORK. SEE ESPECIALLY NIST TRUSTWORTHY EMAIL).**

To work effectively, a firm must implement a strong DMARC policy of p=reject. This policy determines that all unauthorized emails which fail DMARC validation are completely blocked by recipient servers. Traditionally, getting to p=reject can be a complex and time-consuming task, and if done incorrectly, it can leave firms vulnerable to both threats and poor email deliverability.

Red Sift's OnDMARC solves the complexities of DMARC and complies with DORA

Red Sift's flagship product OnDMARC makes up the foundation of our Integrated Email Security and Brand Protection Platform. It was created to help organizations achieve successful deployment of the internationally recognized standard, DMARC, easily and reliably. OnDMARC enables organizations to quickly configure SPF, DKIM, and DMARC for all legitimate email sources and block exact domain impersonation.

ONDMARC

Minimize time to protection

Get to DMARC enforcement in an average time of 4-8 weeks.

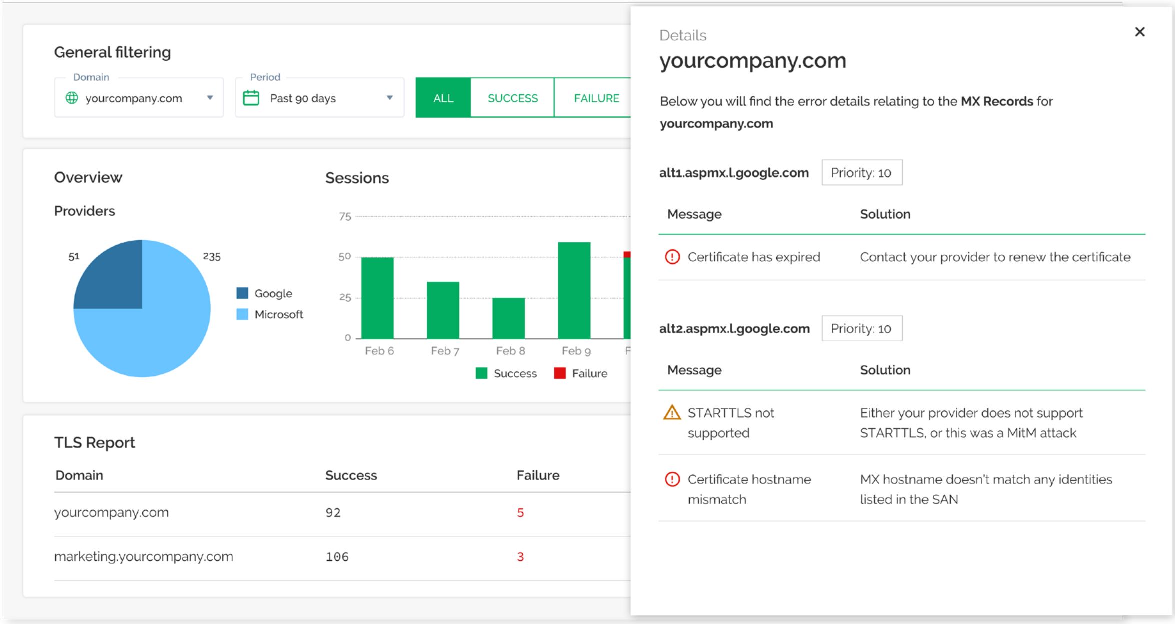
Configure with confidence

Don't worry about your email deliverability being impacted.

Data-driven decision making

Access to the context you need to make smarter choices.

OnDMARC simplifies the otherwise complex deployment of these standards with user-friendly interfaces and clear guidelines. It also enabled the simplified implementation of additional email protocols, BIMI and MTA-STS.



TLS Report

Domain	Success	Failure
yourcompany.com	92	5
marketing.yourcompany.com	106	3

Details

yourcompany.com

Below you will find the error details relating to the **MX Records** for **yourcompany.com**

alt1.aspmx.l.google.com Priority: 10

Message	Solution
Certificate has expired	Contact your provider to renew the certificate

alt2.aspmx.l.google.com Priority: 10

Message	Solution
STARTTLS not supported	Either your provider does not support STARTTLS, or this was a MitM attack
Certificate hostname mismatch	MX hostname doesn't match any identities listed in the SAN

What DORA says:

> *"Financial entities shall use and maintain* ***updated*** *....* ***tools*** *which are:*
>
> ***a. appropriate to the*** *nature, variety,* ***complexity*** *and magnitude of* ***operations****,*
>
> ***b. reliable****,*
>
> *c. have* ***sufficient capacity to accurately process the data*** *necessary for performance of activities and*
>
> *d. technologically* ***resilient to deal with additional information processing****"*
>
> DIGITAL OPERATIONAL RESILIENCE ACT (DORA), ARTICLE 6 (1)

What we say:

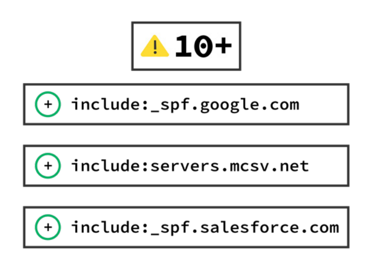
This is a useful provision as it provides real clarity for conformance with DORA with respect to systems, protocols and importantly, tools. With a framework as clear as this, firms have the perfect opportunity to ask their vendors these questions in relation to their own solutions. Vendors also need to be aware that their responses would form part of the firm's decision-making process. These responses could then form part of any due diligence exercise and this paper trail could be relied on if the statement turned out to be untrue (contracts can be rescinded or canceled without liability if this is found to be the case).

This is also an efficient way for firms to eliminate products that cannot perform the necessary functions. It is key that financial firms ensure the systems and tools they're buying adhere to the above framework, and that third-party vendors are clear on what they can and cannot offer.

Reliable and sufficient SPF Management with the Red Sift Platform

SPF stands for Sender Policy Framework. It's an email authentication protocol that acts as a whitelist, outlining the senders authorized to send emails on your behalf. Its aim is to prevent email forgery. But while SPF is a key protocol that enables DMARC to work, its drawback is the 10 SPF lookup limit.

What is the SPF lookup limit?



```
include:_spf.google.com
include:servers.mcsv.net
include:_spf.salesforce.com
```

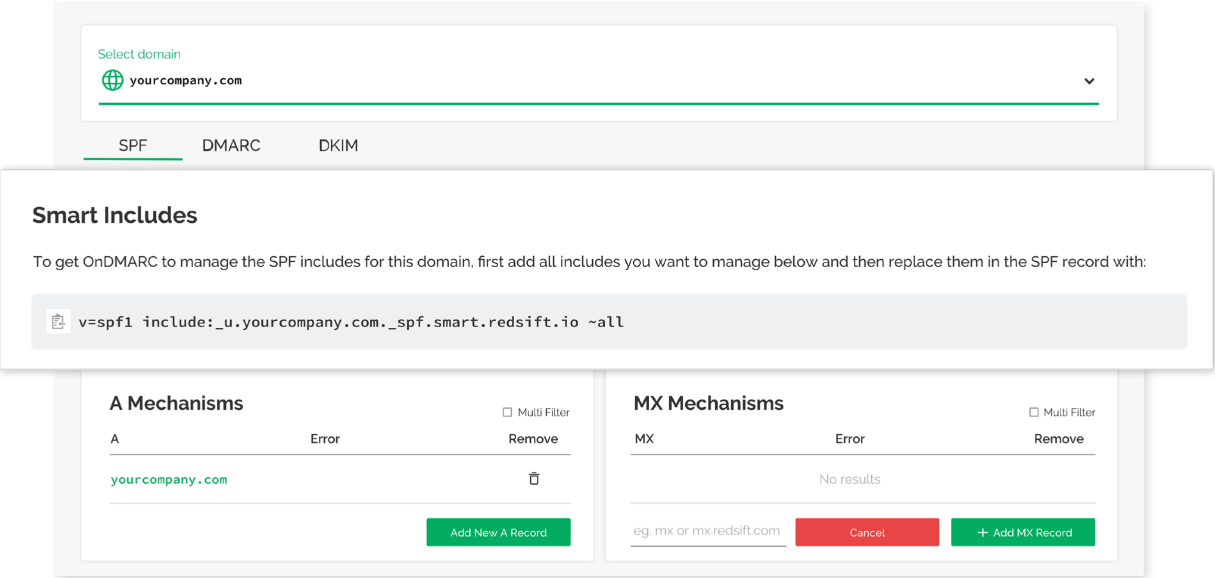
An SPF lookup is when the DNS receiving an email has to 'look up' the IP addresses present in any of the include statements within a record, to check if they match with the IP sending your email. The SPF lookup limit is the number of times a recipient DNS can carry out a lookup for a domain, this is capped at 10 to prevent DDoS attacks.

Most organizations use a number of different mail service providers - G Suite for business emails, MailChimp for marketing emails, Salesforce for customer emails - and each one needs to be added to the organization's DNS in order to authenticate the emails as genuine using SPF. However, this can quickly breach the 10 DNS lookup limit imposed by SPF.

Many DMARC solutions use SPF flattening to manage SPF lookups, meaning they can easily break and this can lead to serious email deliverability issues. These forms of SPF management are unreliable, outdated, and will not comply with DORA.

OnDMARC's *Dynamic SPF* is reliable, resilient, and has sufficient capacity to accurately process the data, thus complying with DORA.

OnDMARC's *Dynamic SPF* was built to be self-healing and cognisant of the reality of the internet. Essentially, it overcomes the 10 lookup limit by enabling organizations to use a single dynamic include statement to combine all authorized services correctly at the point of query. This prevents your authorized traffic from failing SPF validation, regardless of how many sending services you use.



Select domain

yourcompany.com

Smart Includes

To get OnDMARC to manage the SPF includes for this domain, first add all includes you want to manage below and then replace them in the SPF record with:

```
v=spf1 include:_u.yourcompany.com._spf.smart.redsift.io ~all
```

A Mechanisms

□ Multi Filter

A	Error	Remove
yourcompany.com		

MX Mechanisms

□ Multi Filter

MX	Error	Remove
No results		

> *The infrastructure of Dynamic SPF is built on a leading cloud system which provides high-performance data storage and multiple availability zones to manage resilience and failover. Our application stack is often evaluated by larger customers when making a decision. It is actively in use by a number of enterprise customers including Wise (formerly Transferwise), a leading peer-to-peer money transfer platform revolutionizing how money flows around the world. They trust Dynamic SPF to deliver more than 1.5M emails every day.*
>
>
>
> Randal Pinto
> CHIEF TECHNOLOGY OFFICER
> RED SIFT

Step 3. Prioritize protection and prevention

What DORA says:

> *Financial entities shall … procure and implement ICT security strategies … and tools that aim at, in particular, ensuring the* ***resilience, continuity and availability*** *of ICT systems, and maintaining high standards of security, confidentiality and integrity of data … financial entities shall use state of-the-art ICT technology and processes which: (a)* ***guarantee the security of the means of transfer of information****; … (c)* ***prevent information leakage***
>
> DIGITAL OPERATIONAL RESILIENCE ACT (DORA), ARTICLE 8 (2, 3)

What we say:

Businesses rely heavily on email as an important means of transfer of information. 90% of data breaches are a result of weak email security[4], and this fact gives rise to two critical concerns relating to email security for firms that fall within the scope of DORA. Firstly, how is the firm able to detect malicious content in inbound emails? And what mechanism do they have in place to authenticate users on the send side? Do they form part of your business's trusted network or do they just look like they do?

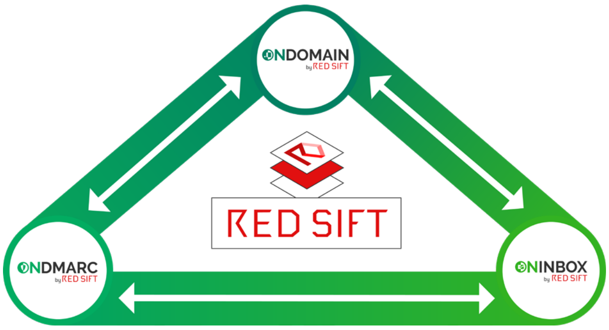
Secondly, we have good information that where criminals rely on lookalike domains to conduct their attack, these domains are purchased within a short period of time before the commencement of the cyberattack - typically within 48 hours. As these domains are purchased with legitimate credit cards, there is rarely an opportunity to detect the spinning up of the lookalike domain without purpose-built software. So how can firms ensure mitigation of these threats?

Protecting transfer of information and preventing data leakage with the Red Sift Platform

> *(3c) prevent information leakage; - a significant number of data breaches are the result of weak email security, so businesses need to be securing email as a priority.*
>
> ROIS NI THUAMA, PHD

The Red Sift Integrated Email Security and Brand Protection Platform is made up of a number of gold-standard and award-winning products: OnDMARC, OnDOMAIN and OnINBOX. These are designed to work in unison to block outbound phishing attacks, analyze the security of inbound emails, and provide domain impersonation defense for company-wide threat protection.

1. **OnDMARC** blocks the most sensitive attack vector: the impersonation of real domains
2. **OnDOMAIN** uncovers and disarms impersonation domains as they are being prepared and before they can reach the inboxes of customers, counterparties, or the wider public
3. **OnINBOX** detects and flags inbound email threats for users, providing protection at the point of interaction



How OnDOMAIN protects you from threats outside your perimeter

Uncover

OnDOMAIN monitors 150 million newly registered domains and subdomains every day making it easy for you to define and visualize complex domain estates.

Investigate

OnDOMAIN paints the full picture of a domain's health and validity to reveal vulnerabilities so you can take action to prevent them.

Take down

OnDOMAIN provides integrated takedown enabled in partnership with industry specialists to defend your brand against abuse and reputational damage.

How OnINBOX supercharges threat detection and response

Move away from a culture of "train and blame"

Empower your users to confidently interact with email.

Uncover subtle threat signals that SEGs miss

Use technology that is always learning and adapting.

Spot suppliers putting your organization at risk

See who is at risk of impersonation in your supply chain.

Step 4. Ensure you can detect threats

What DORA says:

> *Financial entities shall have in place mechanisms to **promptly detect anomalous** activities… Financial entities shall devote **sufficient resources** and capabilities, with due consideration to their size, business and risk profiles, to monitor user activity, occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.*
>
> DIGITAL OPERATIONAL RESILIENCE ACT (DORA), ARTICLE 9 (1, 3)

What we say:

With stopping zero-day attacks and improving domain perimeter protection two increasing priorities for businesses, it's no surprise that DORA dedicates an article to detection. But how can firms successfully detect anomalies and threats and ensure hygiene across their entire email and domain landscape?

Detecting anomalies with the Red Sift Platform

Detection of anomalous activities is integral to all products on the Red Sift platform; it is only through the swift surfacing and contextual analysis of these types of incidents that security-first organizations can take relevant action and deploy incident response.

ONDMARC

OnDMARC detects and surfaces information to its users in a variety of ways, for example detecting misconfigured or missing email protocols, noticing that the reputational score of an email source is in decline, or uncovering shadow IT. OnDMARC's Sender Intelligence feature provides more granular insight into forensic reports too.

ONDOMAIN

OnDOMAIN scans up to 150 million newly-registered hostnames every day, continuously searching to ensure firms stay up-to-date on the emergence of lookalikes and their evolving threat level, and offering fast takedown functionality. This detection functionality is key to uncovering phishing sites before they can be weaponized, making it a key solution in any organization's cybersecurity armory.

ONINBOX

OnINBOX immediately uncovers any malicious attacks in inbound emails (many of which are hiding in plain sight) by using easy-to-understand traffic light indicators. OnINBOX Manager - OnINBOX's admin solution - provides insight into an organization's complete network of connections in one centralized dashboard, so security teams can easily spot potential phishing emails and remediate them.

Step 5. Prepare for response and recovery

What DORA says:

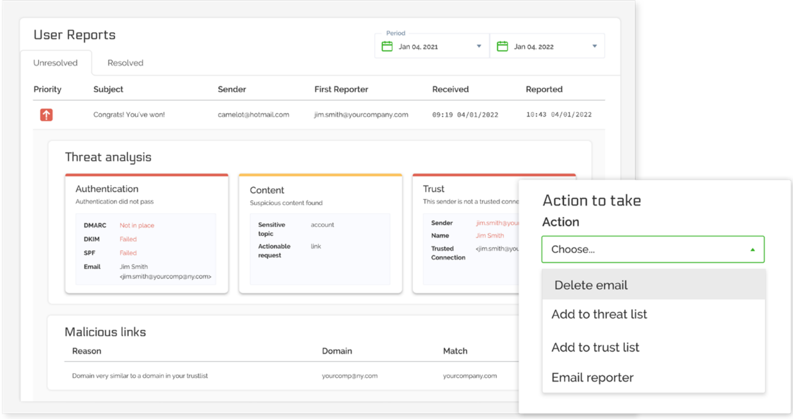
> *Financial entities shall …* **quickly, appropriately and effectively responding to and resolving all ICT related incidents**, *in particular but not limited to cyber-attacks, in a way which limits damage and prioritizes resumption of activities and recovery actions*
>
> DIGITAL OPERATIONAL RESILIENCE ACT (DORA) ARTICLE 10 (2)

What we say:

Having in place the solutions, systems, and plans to respond to and recover quickly from cyberattacks is good common sense for any financial firm. But with the advent of DORA, it's now expected of them. Given the damage and disruption cyberattacks like ransomware and DDoS can cause, it's more important than ever that firms are auditing their capabilities to ensure response and recovery is at the forefront of their priorities in preparation for DORA.

Fast response and recovery with the Red Sift Platform

It's no secret that email phishing and BEC are common causes of successful cyberattacks. As well as employing standardized protocols like DMARC, organizations need to ensure they're taking every step to protect employees, who shouldn't be expected to mitigate attacks on their own.



User Reports

Period: Jan 04, 2021 – Jan 04, 2022

Unresolved | Resolved

Priority	Subject	Sender	First Reporter	Received	Reported
↑	Congrats! You've won!	camelot@hotmail.com	jim.smith@yourcompany.com	09:19 04/01/2022	10:43 04/01/2022

Threat analysis

Authentication
Authentication did not pass

DMARC	Not in place
DKIM	Failed
SPF	Failed
Email	Jim Smith <jim.smith@yourcomp@ny.com>

Content
Suspicious content found

Sensitive topic	account
Actionable request	link

Trust
This sender is not a trusted conne

Sender	jim.smith@you
Name	Jim Smith
Trusted Connection	<jim.smith@you

Malicious links

Reason	Domain	Match
Domain very similar to a domain in your trustlist	yourcomp@ny.com	yourcompany.com

Action to take

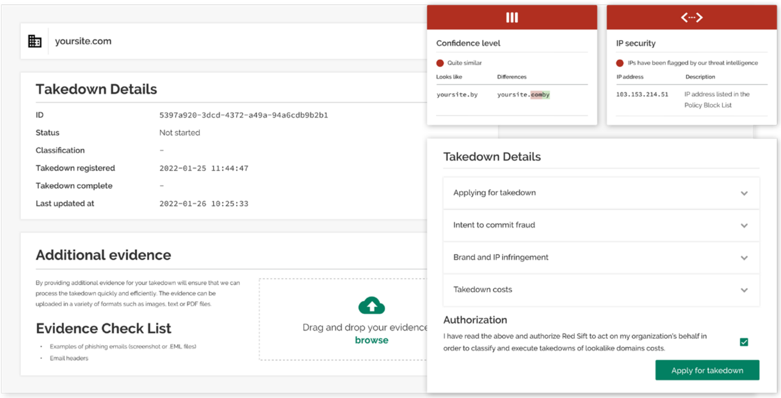
Action: Choose...

Immediate remediation of potential phishing emails with OnINBOX

Not only does OnINBOX flag otherwise impossible-to-spot risks to the naked eye, it also provides an easy way for employees to report potential risks, improving ICT response times. After an email has been reported and reviewed, the response team can delete and block from within the OnINBOX Manager interface. The solution helps response teams focus on the most pressing threats first with a prioritized queue of reported emails.

One-click takedown of phishing websites with OnDOMAIN

Working coherently with the above, OnDOMAIN enables takedown of phishing websites (in partnership with industry specialists) to defend your brand against abuse and reputational damage. As OnDOMAIN is able to spot lookalike domains on day zero and speedily take them down, it limits damage and prioritizes resumption of activities and recovery actions.



yoursite.com

Takedown Details

ID	5397a920-3dcd-4372-a49a-94a6cdb9b2b1
Status	Not started
Classification	–
Takedown registered	2022-01-25 11:44:47
Takedown complete	–
Last updated at	2022-01-26 10:25:33

Additional evidence

By providing additional evidence for your takedown will ensure that we can process the takedown quickly and efficiently. The evidence can be uploaded in a variety of formats such as images, text or PDF files.

Evidence Check List

- Examples of phishing emails (screenshot or .EML files)
- Email headers

Confidence level

● Quite similar

Looks like	Differences
yoursite.by	yoursite.comby

IP security

● IPs have been flagged by our threat intelligence

IP address	Description
103.153.214.51	IP address listed in the Policy Block List

Takedown Details

Authorization

I have read the above and authorize Red Sift to act on my organization's behalf in order to classify and execute takedowns of lookalike domains costs. ☑

Step 6. Manage your exit strategies

What DORA says:

> *Financial entities* ***shall put in place exit strategies*** *in order to take into account risks that may emerge at the level of ICT third-party service provider, in particular a possible failure of the latter, a deterioration of the quality of the functions provided, any business disruption due to inappropriate or failed provision of services or material risk arising in relation to the appropriate and continuous deployment of the function.*
>
> DIGITAL OPERATIONAL RESILIENCE ACT (DORA), ARTICLE 25 (9)

What we say:

Until now, financial firms have been at the mercy of any unscrupulous third-party ICT vendors that want to prolong the lives of the products and contracts they offer. This is because they have been allowed to provide their offering with no clear exit strategy once a contract is up, meaning firms are often lumbered with kit that is not fit for purpose, but would cause too much business disruption to remove.

DORA changes this, and now clear exit strategies must be put in place by financial firms and ICT providers, meaning the power is handed back to the consumer (in this case, the financial firms).

Book your Red Sift Platform demo today

It should come as no surprise that, in our eyes, DORA is long overdue. Businesses deserve clear and comprehensive guidance on how they can mitigate the ever-expanding cyber threat landscape. DORA is here to make lives easier, and businesses better. Plus, it's not just financial firms and third-party software providers that can benefit, sectors of all shapes and sizes can listen to what DORA says, and use its guidance to make their organizations better, faster, and stronger.

Ultimately, DORA isn't asking firms to see around corners. Instead, it expects them to see the writing on the wall (i.e. what is reasonably foreseeable, and what is avoidable) and address this with something that's proportionate and affordable.

At Red Sift, we don't create solutions to fix every problem. Instead, we look to address the most significant cyber threats facing organizations of all sizes. We listen to the experts and look to best practices in everything we do, and we know that for cybersecurity to work we all need to play our part. We call this democratizing cybersecurity for all, and our platform exists to ensure this.

Find out how the Red Sift Platform can help your business mitigate risks relating to email and domain security, and help you get ready for DORA.

BOOK YOUR FREE RED SIFT PLATFORM DEMO TODAY

RED SIFT

About Red Sift

Red Sift enables security-first organizations to successfully communicate with and ensure the trust of their employees, vendors, and customers. As the only integrated cloud email and brand protection platform, Red Sift automates BIMI and DMARC processes, makes it easy to identify and stop business email compromise, and secures domains from impersonation to prevent attacks.

Founded in 2015, Red Sift is a global organization with international offices in the UK, Spain, Australia, and North America. It boasts a client base of all sizes and across all industries, including Domino's, Telefonica, Pipedrive, Rentokil, Wise, and top global law firms. Find out how Red Sift is delivering actionable cybersecurity insights to its global customers at redsift.com.

References

1. Companies Act 2006, section 174
2. Security Scorecard
3. National Institute of Standards and Technology Trustworthy Email SP 800-177 Rev. 1
4. CISCO's 2021 Cybersecurity Threat Trends report

Rois Ni Thuama, PhD.,
Digital Operational Resilience Act (DORA)
National Institute of Standards and Technology (NIST)