REPORT

DORA and Cyber Risk:

A New Framework for Third-Party Risk in the European Union

Security Scorecard

Contents

Introduction

In January 2023, a landmark law in the European Union [EU] on the cybersecurity of the financial services sector entered into force. The Digital Operational Resilience Act (DORA) requires banks, other financial entities, and some ICT third-party providers in the EU to implement a series of cybersecurity-related measures intended to protect consumers and shore up the EU's financial system against systemic risks arising from the central role that information and communication technologies (ICT) play in the provision of financial services.

DORA builds on over a decade of global and EU efforts to address systemic risks to financial stability in the aftermath of the 2008 global financial crisis. In 2017, the European System Risk Board (ESRB) chartered a European Systemic Cyber Group (ESCG) to examine systemic cyber risks in the EU. That study examined cyber risks in the context of other risks to financial stability, including credit, market, liquidity, and operational risks.[1] It identified characteristics of cyber risk that differentiate it from these other risks, specifically the speed and scale of adversarial cyber threats that result from complex risk interdependencies among market actors. The study also concluded that these interdependencies mean that the risk exposure of any single financial entity affects other financial entities, ICT vendors, and other third parties—and that adverse risk outcomes can cascade in ways that threaten the overall financial system.

At its core, systemic risk is about trust. DORA is an effort to build resilience within the financial service sector by requiring financial services organizations to establish and monitor networks of trust amongst themselves and their ICT vendors. However, trust requires verification through monitoring and transparency (to paraphrase the Russian proverb). As financial regulators in the EU member states develop their national implementation laws for DORA, they should familiarize themselves with the innovative, cost-effective risk transparency and verification ecosystem available to organizations subject to DORA. Financial entities subject to DORA can take steps now to manage third-party risk more effectively.

1. "Systemic Cyber Risk," European Systemic Risk Board, February 2020.

DORA HIGHLIGHTS

- Covers EU financial entities and their ICT vendors.
- Requires firms to implement a risk management framework, identify "critical and important functions," map assets and dependencies, and make senior executives accountable for cyber risk decisions.
- Covered firms must classify and report certain cyber incidents to relevant authorities.
- Establishes a testing and oversight regime for monitoring risk resilience performance.
- Financial entities must manage third-party risk.

Cyber attacks and vulnerabilities put the EU Financial System at risk

On January 31 2023, the cleared derivatives unit of Dublin-based ION Trading Technologies Ltd.—whose software automates the clearing of derivatives trades–suffered a ransomware attack and had to pull its systems offline. This forced financial entities to confirm trades manually and regulators to delay the issuance of market-moving reports.[2] It also highlighted for business leaders and regulators how one organization's decisions–in this case, the ICT vendor ION—can give rise to systemic risks. As Fabio Panetta, a member of the European Central Bank's Executive Board, observed in the aftermath:

> The financial ecosystem's reliance on third-party products and services is a key risk, especially when financial entities outsource critical functions to them. An attack on these third parties or on their products and services can disrupt and harm the financial infrastructures that rely on them, with spillovers to interconnected entities. When such third-party products and services are widely used in the financial ecosystem, a cyberattack can have widespread, possibly systemic effects by having an impact on multiple financial entities at once.[4]

2. James Rundle, "Cyberattack on ION Derivatives Unit Had Ripple Effects on Financial Markets," The Wall Street Journal, February 10, 2023.
3. "The Quick and the Dead: building up cyber resilience in the financial sector," Introductory remarks by Fabio Panetta, Member of the Executive Board of the ECB, at the meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, March 8, 2023.

The ION case is the latest entry in a growing roster of cyber incidents involving the financial services sector.

- In 2011-2012, Iran carried out a campaign of distributed denial of service (DDoS) attacks against American banks in apparent retaliation of U.S.-led economic sanctions relating to Iran's nuclear program.
- In 2016, hackers widely believed to be affiliated with the North Korean government hacked into the Bank of Bangladesh and used the bank's SWIFT credentials to steal $81 million from its Federal Reserve Bank of New York account.[4]
- Russia's NotPetya cyberattack on Ukraine in 2017 brought down the IT infrastructure of thousands of victims globally, including at least 22 banks in Ukraine alone at astonishing speed (one bank reported its systems were destroyed within 45 seconds of the attack's start).[5] This incident highlights how third-party risk can have devastating consequences: the attack began with Russia compromising software used by companies doing business in Ukraine to file tax information.
- VISA's payments network suffered a 10-hour outage in June 2018 that caused 10% of transactions–$5.2 million–to be declined.[6] Five weeks later, MasterCard suffered an outage.[7]
- More recently, a survey of 130 global financial entities found that nearly three-quarters had suffered a ransomware attack in 2022.[8]

Software vulnerabilities in the ICT products used by financial entities are an especially significant source of cyber risk because such vulnerabilities can put an entire user base at risk. Infosec veterans will recall the Herculean, multi-year Y2K effort to ensure that digital systems survived the transition to the new millennium. That was a case where industry had advance warning and could—and did—prepare for years in advance: the New York Stock Exchange, for example, reportedly began preparing in 1987 with an investment of $29 million and a team of 100 programmers.[9]

Today, vulnerabilities with global reach that affect millions of users emerge with disheartening regularity and without advance warning (see Figure 1). For example, consider the third-party breaches that resulted recently from the Cl0p ransomware group's widespread exploitation of CVE-2023-34362, a vulnerability in the MOVEit managed file transfer solution. The MOVEit exploit illustrates the risks that EU firms face when financial service providers use vulnerable software. Zellis, a payroll provider serving both UK and EU organizations, was one of the campaign's earliest and most prominent victims to be publicly identified after the vulnerability's initial disclosure on May 31. The threat actors' targeting of Zellis's vulnerable MOVEit instance resulted in the theft of at least eight customer organizations' data, including prominent organizations such as Aer Lingus, British Broadcasting Corporation, British Airways, and Boots.[10]

4. Kim Zetter, "That Insane, $81M Bangladesh Bank Heist? Here's What We Know," Wired, May 17, 2016.
5. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," August 22, 2018.
6. Letter from Visa to The Rt Hon. Nicky Morgan MP, June 15, 2018..
7. Martin Arnold, "MasterCard customers suffer outages around the world," July 12, 201.
8. Gillian Tett, "The Financial System Is Alarmingly Vulnerable to Cyber Attack," February 16, 2023.
9. Eric Andrew-Gee, "Y2K: The strange, true history of how Canada prepared for an apocalypse that never happened, but changed us all," The Globe and Mail, June 1, 2020.
10. Carrie Pallardy, "Payroll Provider Zellis Falls Prey to MOVEit Transfer Breach," Information Week, June 9, 2023.

SecurityScorecard launched an investigation into the Zellis compromise in response to the initial reports. This research revealed alarming insights about the scale and persistence of the attack. Our analysis indicated that data theft occurred in several steps:

1. **Initial SQL injection scanning**
2. **Another test to verify the vulnerability**
3. **Exploitation of the vulnerability via SQL injection**
4. **A reverse HTTP connection from Zellis's affected IP back to the adversary's infrastructure with a large data transfer**

SecurityScorecard collected network flow (NetFlow) data from Zellis-attributed IP ranges, which indicated large outbound transfers over HTTPS, suggesting the presence of a web shell like the one observed in some of ClOp's attacks against vulnerable MOVEit services. Additionally, SecurityScorecard researchers detected exfiltration over SSH to known malicious IP addresses. By leveraging SecurityScorecard's Attack Surface Intelligence module, the team was able to identify vulnerable Zellis-attributed IP addresses hosting MOVEit servers within minutes and, by combining Attack Surface Intelligence with NetFlow data, the SecurityScorecard team was further able to identify the exact attack vector against Zellis's affected IP.

Zellis is, however, just one among many victims of the campaign exploiting CVE-2023-34362 and related MOVEit vulnerabilities. The SecurityScorecard Threat Research, Intelligence, Knowledge, and Engagement (STRIKE) Team's subsequent analysis identified a wider network of malicious infrastructure likely involved in the campaign, which may reveal a broader pattern of activity targeting organizations in sectors including professional services, retail, communications, transportation, energy, and government.

Understandably, the outlook among chief risk officers at banks is grim: 72% cited cyber risk as their top risk priority for 2023-2024 in EY/IIF's annual global bank risk management survey.

72% of chief risk officers at banks cited **cyber risk as their top risk priority** for 2023-2024

11. Carrie Pallardy, "Payroll Provider Zellis Falls Prey to MOVEit Transfer Breach," Information Week, June 9, 2023.
12. "Three Steps to Prevent a Cybersecurity Breach from MOVEit Exploit," SecurityScorecard, June 7, 2023.
13. "MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response," Huntress Labs, June 1, 2023.
14. "SecurityScorecard Identifies Infrastructure Linked to Widespread MOVEit Vulnerability Exploitation," SecurityScorecard, June 20, 2023.
15. "How Bank CROs Are Responding to Volatility and Shifting Risk Profiles, EY, January 10, 2023.

FIGURE 1

SOFTWARE VULNERABILITIES AND THIRD-PARTY RISK

- Heartbleed (2014) is a critical vulnerability in the OpenSSL cryptographic software library. This vulnerability allowed an attacker to steal sensitive information from affected systems, including passwords and encryption keys.
- Shellshock (2014) was a vulnerability in Bash shell, allowing unauthorized code execution on vulnerable systems. Meltdown and Spectre (2018) are two separate but related security vulnerabilities in computer processors. If exploited, attackers could access sensitive data stored on or processed by the computer.
- EternalBlue (2017) refers to an exploit of a zero-day vulnerability in the Server Message Block (SMB) protocol. It was used by North Korea and Russia (respectively) in the WannaCry (2017) and NotPetya (2017) attacks.
- Apache Struts (2017) had a critical vulnerability in its web application framework, allowing hackers to execute arbitrary code on infected systems. Threat actors exploited this vulnerability to infiltrate Equifax (2017) and expose the personal information of over 145 million people.
- BlueBorne (2017) is a Bluetooth vulnerability affecting various devices, allowing remote code execution and potential device takeover.
- KRACK (2017) involved weaknesses in the Wi-Fi encryption protocol WPA2 that could enable attackers to intercept and decrypt data.
- Sandworm (2017) is a vulnerability in the Microsoft Windows Object Linking and Embedding (OLE) technology that allows hackers to execute arbitrary code on infected systems. The Sandworm vulnerability was exploited in a cyberattack against Ukraine in 2017, among other examples.
- SolarWinds (2020) refers to the company whose popular suite of IT monitoring and management products called Orion was subverted by a threat actor, giving the actor unauthorized access to tens of thousands of organizations ranging from U.S. government agencies to major multinational firms.
- ProxyLogon (2021) are a series of four zero-day vulnerabilities discovered in Microsoft Exchange that allow attackers to remotely execute code and gain unauthorized access to Microsoft Exchange servers.
- ProxyShell (2021) is a set of vulnerabilities in Microsoft's Exchange Management Shell that allow attackers to execute arbitrary code on Exchange servers.
- PrintNightmare (2021) is a Windows Print Spooler service vulnerability that allows attackers to take control of vulnerable systems.
- Log4j (2021) is a critical security flaw discovered in the Apache Log4j logging library that allows attackers to remotely execute malicious code.
- Follina (2022) is a vulnerability in Microsoft Office that allows attackers to execute arbitrary code on vulnerable systems through a malicious Office document.
- MOVEit (2023) refers to a zero-day SQL injection flaw in the MOVEit managed file transfer software, enabling unauthorized data access.

A Closer Look: How the Largest EU Financial Entities Fare

To provide insight into the cybersecurity vulnerabilities the financial markets face leading up to the implementation of DORA in January 2024, SecurityScorecard data scientists studied a cohort of financial institutions using our security ratings platform.

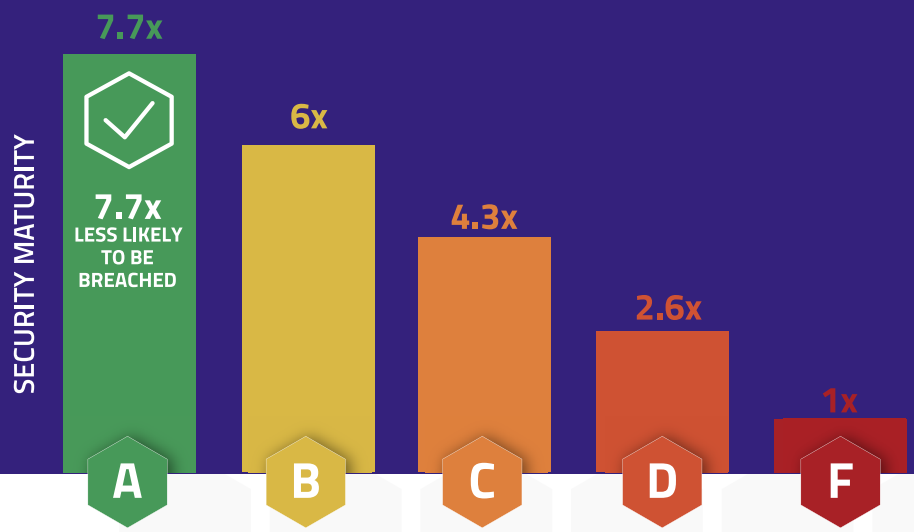
We examined the cybersecurity profiles of the largest 240 financial institutions, including their third- and fourth-party vendor operations in the EU in 2023. This aggregates into an ecosystem of 26,142 domains. The top 240 were determined by current revenue, assets under management, or gross written premium. These 240 institutions included Private Equity, Asset Management, Retail Banks, Insurance and Pension Funds.

This financial institution ecosystem was scored and analyzed against reported data breaches to demonstrate the cybersecurity posture of the financial market in the lead up to the full implementation of DORA in January 2024. The SecurityScorecard platform scores domains on 10 security categories (network security, DNS health, patching cadence, cubit score, endpoint security, IP reputation, web application security, hacker chatter, leaked credentials, and social engineering) to obtain an indicator of an institution's cybersecurity profile. Based on these 10 factors, we assigned an overall grade to each institution and their third parties to demonstrate at-a-glance how secure a company is relative to the rest of their industry.

Our intelligence is the result of daily scans of the entire internet to map cybersecurity risk exposure and bring transparency to an organization's cyber hygiene. SecurityScorecard does this without going behind any firewalls, only collecting public-facing data. SecurityScorecard offers an "outside-in" perspective on an organization's security posture: we give organizations the ability to see what a hacker would see and are thus able to generate insights about the vulnerabilities, active exploits, and advanced cyber threats that a specific organization faces. Our customers use the platform not only to identify weaknesses in their own enterprise cyber hygiene, but to support their vendor risk management and supply chain security initiatives as well.

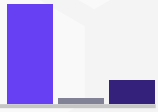
SecurityScorecard generates security ratings by drawing on publicly available information, weighted and combined with historical data, to produce an objective security score. Importantly, this score, and the analytics behind it, change dynamically in response to changes in an organization's exposure to risks: if an organization's cyber hygiene starts to deteriorate, its score will suffer. While a high score does not translate to immunity from cyber risk, poor scores are correlated with an increased likelihood of a breach. This is unsurprising, as a poor score reflects that an organization has not sufficiently hardened its infrastructure against malicious actors.

Companies with a Better Security Rating are More Resilient



We found that 18% of the cohort of 240 financial entities studied had a grade of C or lower on our A-F grading scale.

All financial institutions

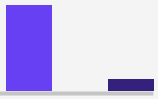


78% have experienced a third-party data breach in the past year

4% have been breached on their own domain in the last year

18% of 240 of Europe's largest financial institutions have a C rating or below

Private Equity



67% have experienced a third-party data breach in the past year

0% have been breached on their own domain in the last year

9% have a C rating or below

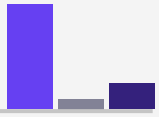
Asset Management

68% have experienced a third-party data breach in the past year

4% have been breached on their own domain in the last year

21% have a C rating or below

Retail Banks

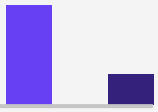


82% have experienced a third-party data breach in the past year

8% have been breached on their own domain in the last year

20% have a C rating or below

Insurance Firms

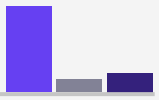


78% have experienced a third-party data breach in the past year

0% have been breached on their own domain in the last year

24% have a C rating or below

Pension Funds



67% have experienced a third-party data breach in the past year

10% have been breached on their own domain in the last year

15% have a C rating or below

Our findings reveal a ceiling for the state of risk resilience among financial entities in the EU: our survey examined the largest financial entities in the EU, which also tend to have the most resources to devote to cyber risk resilience. If 18% of the most well-resourced financial entities in the EU have grades of C or worse (making them 4 to 7 times more likely to suffer a breach than the most prepared organizations), then it's likely that the overall cyber resilience for other financial entities is much lower.

In light of these risks, the EU's focus on financial systems resilience against cyber threats is understandable.

4 to 7x
more likely to suffer a breach

Third and fourth party cybersecurity breaches pose significant risk for the EU

In its 2020 report on systemic cyber risk, the ESCG warned that a "cyber incident can evolve into a systemic crisis when trust in the financial system is eroded." Trust in the system is relational: it exists when individual entities in the financial system and their stakeholders (such as customers and investors) believe that the system will continue to enable the delivery of what is owed to them by others in the system, such as funds in a depository account, access to credit or liquidity, or insurance coverage. We have learned through experience over the past decade that cyber risks are among the factors that can prevent a financial entity from meeting its obligations to stakeholders. As the ESCG further explains, a cyber incident becomes systemic when it disrupts "critical functions supporting the real economy or the generated (or anticipated) financial losses from the incident need to reach a level where the financial system is no longer able to absorb the shock."

In its 2020 report on systemic cyber risk, the ESCG warned that a **"cyber incident can evolve into a systemic crisis when trust in the financial system is eroded."**

DORA is usually described as having five main elements (ICT risk management; incident reporting; digital operational resilience testing; ICT third-party risk; and information sharing). However, its requirements are usefully boiled down to this: how to ensure that financial entities and their ICT vendors internalize the costs of their risk decisions, as opposed to passing them off to customers, business partners, and the broader financial system. Whenever people or organizations are in a position to make risk decisions knowing that they won't bear the full downside risks of those decisions, they will engage in riskier behavior–a problem in economics known as moral hazard.

Threat actors are getting faster and better at scaling their cyberattacks with the help of innovative hacking tools and business models, such as adversarial automation, attack "as a service" offerings from criminal groups, and, increasingly, using attacks on third-party vendors as an access point for compromising vendors' customers and business partners. The majority (54%) of organizations reported a breach originating from a connection to a third-party vendor.[16]

Who financial entities choose to trust and how they sustain that trust are essential factors for the resilience of the EU's financial services sector. According to our data, 78% of the financial entities in our survey were exposed to cyber risk by a breach of a third-party and 84% were exposed by a breach of a fourth party. This exposure is the result of breaches affecting just 4% of financial entities' vendors, highlighting how impactful to the sector as a whole even a relatively small number of breaches can be.

78% of the financial entities in our survey were exposed to cyber risk by a breach of a third-party

84% were exposed by a breach of a fourth party

16. "Report: 54% of organizations breached through third-parties in the last 12 months", Venture Beat, September 2022.

A Verification Framework for DORA

Managing third-party risk is a core theme of DORA, and indeed the EU's approach to digital risks more broadly. DORA requires financial entities to identify and assess all third-party risks. This includes risks to the confidentiality, integrity, and availability of data and systems, as well as risks to the financial entity's ability to continue operating in the event of a third-party incident. Financial entities must implement appropriate mitigation measures, which may include contractual arrangements, technical controls, and operational procedures. They must also monitor and review third-party risks on an ongoing basis to verify that the mitigation measures remain effective and identify new risks or problem areas. Financial entities must report certain information about their third-party risk management to their supervisors, including the nature and extent of the financial entity's reliance on third parties, the results of the financial entity's risk assessments, the mitigation measures that the financial entity has implemented, and the results of the financial entity's monitoring and review activities.

DORA's emphasis on verification through transparency and continuous monitoring reflects a global trend in digital risk management, with the EU at the forefront. For example, in 2022, the G7 issued a set of guidelines that financial institutions can use to manage the cyber risks associated with their third-party relationships. The guidance "G7 Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector" is based substantially on DORA, and echoes its key themes.[17] Cyber risk is a shared responsibility for financial entities and their third-party vendors, who must work together to manage cyber risk. Due diligence is essential: financial institutions must perform due diligence on their third-party vendors to assess their security posture and compliance with relevant contractual and regulatory requirements. Monitoring and remediation must be performed continuously because the cyber risk environment is constantly evolving. And communication is key: financial entities must communicate with their third-party vendors and supervisors about cyber risk to share information and best practices.

These threads about third-party risk and the importance of verification run through the EU's growing corpus of digital risk resilience laws and policies. For example, the EU's NIS2 Directive and the EU Cybersecurity Act require organizations to identify and assess third-party risks on an ongoing basis and to take steps to mitigate these risks. EU Member States are also acting at the national level. The French cyber audit law (Loi n°2022-206 du 14 mars 2022 visant à renforcer la sécurité des systèmes d'information et de communication), for example, requires certain organizations in France to undergo regular cybersecurity audits and manage third-party risk.

> DORA's emphasis on verification through **TRANSPARENCY** and continuous monitoring reflects a global trend in digital risk management, with the EU at the forefront.

However, companies need help managing their third-party risk. In a recent Forrester survey of 800 enterprise risk management decision-makers, 75% reported that their third-party risk management program is done through a manual process.[18] This often includes managing their third-party risk management program through static spreadsheet-based assessments. Manually identifying, assessing, and validating answers from vendors takes up a lot of time and does not scale. An organization must balance limited resources, security talent, and the factors they can control to minimize risk. The emergence of new cybersecurity strategies, like zero trust, can help provide frameworks for this problem, but falls short on implementation and application to make these policies actionable.

17. "G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector," October 2022.
18. The State of Third-party Risk Management: The Not So Subtle Art of Keeping All Balls in the Air, Forrester Research, October 2022.

Seven Steps To Prepare for Dora

Financial entities and their supervisors need a trusted view of security risk. Although DORA doesn't go into full effect until January 2025, third-party risk exists today. Financial entities cannot afford to wait and should consider taking the following actions now to strengthen their resilience against third-party risks:

1. Use the right tools to manage third-party cyber risk. Cyber risk ratings can provide financial institutions with an objective measure of an organization's cybersecurity posture, helping to inform regulatory decisions, reduce the risk of cyber incidents, and effectively comply with regulations, such as DORA in the EU.
2. Speak the language of your stakeholders by clearly communicating and quantifying the success of your third-party risk management program to the regulators, Boards, and C-Suite, with measurable cyber risk ratings.
3. Increase trust and transparency for your organization by showcasing your commitment to continual security improvement with your third parties, highlight your industry certifications and compliance badges in a secure repository that can even drive new business for your organization.
4. In order to stay ahead of adversarial threats, keep pace with the ever-growing network of third parties, and use technology to automate the way they make trusted, data-driven decisions about their vendor risk tolerance.
5. Rapidly surface critical vulnerabilities from third and fourth parties and their products, using business intelligence to automatically reveal the entire digital supply chain.
6. Get ahead of malicious activity with actionable intelligence of any vendor's attack surface, allowing tracking of adversarial behavior, identification of critical vulnerabilities, and defending against active attacks within the entire business ecosystem.
7. Save time by partnering with proven cyber threat experts to transform your current program, improve operational efficiencies, bolster security posture, increase return on existing investments, and completely minimize vendor risk.

Supervisors should familiarize themselves with the innovative, cost-effective risk transparency and verification ecosystem available to organizations subject to DORA. For decades, a common measurement methodology in IT risk management has been the color-coded stoplight scheme, where the color "green" next to a performance requirement signifies having met the requirement, "yellow" signifies partially met, and "red" signifies not met.

In today's threat environment, this simply isn't good enough. Policymakers and business executives should demand greater fidelity about the security postures of the organizations that affect them, whether it's a regulated entity, their own organization, or a third-party partner (such as a supplier). Data and measurement methodologies exist that can empower leaders to better understand their risk exposure and the options and tradeoffs for reducing it.

How SecurityScorecard can help

SecurityScorecard is the trusted, must-have standard for measuring cybersecurity, with over 12 million companies continuously rated. Our platform offers a comprehensive solution covering all major aspects of DORA, including ICT risk management, resilience testing, incident reporting, and third-party risk management. Organizations are empowered to identify and mitigate risks before they become incidents, and with continuous monitoring and vendor risk management, businesses can stay informed about potential threats and vulnerabilities.

We can help you prepare for DORA.
VISIT SECURITYSCORECARD.COM

CONTACT US

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com
United States: (800) 682-1707
International: +1(646) 809-2166