Future of Payments

JOURNAL OF FINANCIAL SERVICES

PUBLISHED BY: **PROJECTIVE GROUP INSTITUTE**

01
2025

Projective
INSTITUTE

JOURNAL OF FINANCIAL SERVICES

Future of Payments

Contents

8 **A launchpad for Payments innovation: the renewed RTGS service**
Victoria Cleland, Chief Cashier and Executive Director for Payments, Bank of England

16 **Payments are in change: where is the journey heading?**
Carlos Nasher, Managing Partner, Thede Consulting (part of Projective Group)
Robert-Jan Wekking, Group Practice Lead Payments, Projective Group

32 **Smarter payment algorithms for liquidity-saving in RTGS: a practitioner's guide**
Jean-Paul Lam, Associate Professor of Economics, University of Waterloo, and Chief AI of Research, Goodlabs Studio
Thomas Lo, CEO and Co-Founder, GoodLabs Studio
Donald McGillivray, Lead Applied AI Developer · GoodLabs Studio
Chris McMahon, Director, AI & Emerging Technologies Research, GoodLabs Studio
Alex Ostrovsky, AI Advisor, GoodLabs Studio

42 **Stablecoins: a new technology, or older than the Knights of Templar?**
Paul H. Kupiec, Senior Fellow and Arthur F. Burns Chair in Financial Policy, American Enterprise Institute

46 **Impact of new technologies on the cash management competitive landscape**
Koen Vierendeels, Head of Transaction Banking, Belfius
Robert-Jan Wekking, Group Practice Lead Payments, Projective Group

54 **The evolution of customer interaction and future expectations**
Jorissa Neutelings, Chief Digital Officer, ABN AMRO Bank N.V.

58 **Issuing and investing in tokenized financial assets: what to look out for and why**
Phoebus L. Athanassiou, Senior Lead Legal Counsel, European Central Bank, and Associate Professor, Goethe Universität, Frankfurt am Main

66 **Cross-border Payments beyond 2027: how to crack speedy progress**
Magali Van Bulck, Head of Public Policy (EMEA), Wise

72 **The future operating model for Payments**
Stephen Peters, Head of Enterprise Payment Solutions, FIS
Alan Verschoyle-King, U.K. Payments Practice Lead, Projective Group

86 **Regulating retail Payments: balancing the competing interest**
Emanuel van Praag, Professor of Financial Technology (FinTech) and Law, Erasmus School of Law, and Counsel, Kennedy Van der Laan

98 **From bottleneck to breakthrough: transforming payment investigations into competitive advantage**
Galitchenko Iouri, Global Products and Markets Manager, SWIFT

102 **Towards European sovereignty in retail Payments**
Diederik Bruggink, Senior Director, Payments, Digital Finance and Innovation, European Savings and Retail Banking Group (ESBG)
Douglas Lockhart, Payments and Digital Finance Advisor, European Savings and Retail Banking Group (ESBG)

110 **The future of Payments: quo vadis Europe?**
Christophe Bonte, Senior Policy Adviser, European Banking Federation

120 **Tackling authorized push payment (APP) fraud: a challenging and evolving Payments environment**
Piers Reynolds, Partner, Freshfields LLP
Laura Feldman, Barrister, Freshfields LLP, and Lecturer in Law, University of Oxford

128 **Challenges for banks: e-wallets and the application of strong customer authentication**
Jan Jans, Partner, RegCounsel Financial Services

136 **Data management and its impact on industry**
John A. Bottega, President, EDM Association

142 **Cashless future - reality or fiction?**
Tobias Trütsch, Managing Director and Head of the Center for Financial Services Innovation (FSI-HSG), University of St. Gallen (HSG), Switzerland

148 **Preparing for October 2025: implementation and impact of the EPC's Verification of Payee scheme**
Dominique Allebroeck, Product Manager, The European Payments Council

154 **Protecting self-hosted payment systems against ransomware: a comprehensive guide**
Buck Rogers, Professor in Cyber Security, University of Gloucestershire, and Cyber Advisor, Projective Group
Scott Beange, Head of Data Management and Cyber Strategy, Projective Group

162 **Transforming cross-border Payments: navigating technological innovation, geopolitical fragmentation, and auditing challenges**
David S. Krause, Emeritus Associate Professor of Finance, Marquette University
Eric P. Krause, Assistant Professor of Accounting, Iowa State University

176 **CBDCs and the digital euro: AML compliance moves closer to the end-user**
Christian Sillaber, Senior Researcher, Department of Private Law, University Bern

Dear reader,

Welcome to this, the inaugural edition of the Projective Group Institute's new Journal of Financial Services!

We're very excited to be launching our Journal at a time of immense challenge and change for the financial services industry, and we've drawn upon the deep subject matter expertise of the many renowned contributors to this edition of the Journal to bring you what we hope you'll find to be a highly stimulating series of articles.

We'll be publishing editions of the Journal on a regular basis, and each time we will be focusing on those topics our Advisory Board members, who are leading academics and executives, are telling us are of key strategic importance to them. And it's for that reason that we've chosen to focus this edition on the world of Payments.

Payments has gone from being an often-overlooked, quite slow-changing, typically back-office, function to becoming one of the most transformed - and transformative – functions in the financial services industry. And all of that has happened within the space of only a few years. Digitization, cloud native technology, financial crime and fraud, artificial intelligence, and many other recent developments, combined with ever-greater regulatory scrutiny and ever-increasing client expectations, have created the perfect storm for legacy Payments providers and have opened this area up to newer and more agile competitors.

We focus on the drivers of that transformation, the implications of those drivers for the various players in the Payments value-chain, and the key decision points firms will therefore soon face if they intend to remain leaders in this field.

I'm conscious that in creating the articles in this Journal, many individuals have spent many hours researching and writing, and I'm very grateful for their time and expertise!

I look forward to getting your feedback on our new Journal of Financial Services, and to speaking with you again soon.

Stefan Dierckx, Founder & CEO, Projective Group

Future of Payments

Protecting self-hosted payment systems against **ransomware**: a comprehensive guide

Buck Rogers,
Professor in Cyber Security, University of Gloucestershire, and Cyber Advisor, Projective Group

Scott Beange,
Head of Data Management and Cyber Strategy, Projective Group

ABSTRACT

This paper explores the growing threat of ransomware to self-hosted payment systems, which are increasingly targeted due to the sensitive financial data they handle and their operational importance. It examines the evolving tactics used by ransomware actors, including double extortion and backup destruction, and identifies common vulnerabilities in payment infrastructure such as weak access controls, unpatched systems, and insufficient segmentation. Drawing on industry best practices and peer-reviewed research, this article outlines a multi-layered defense strategy incorporating strong access controls, endpoint protection, immutable offline backups, staff training, and incident response planning. It also stresses the importance of threat intelligence and compliance with standards like PCI DSS. The paper concludes with actionable recommendations to help financial organizations enhance resilience, minimize operational disruption, and reduce the likelihood of ransom payments.

1. Introduction

The evolving sophistication of ransomware tactics necessitates a proactive approach, including strategies for mitigating cloud-based ransomware threats [Dopamu (2024)].

Ransomware, a form of malicious software that operates by encrypting data on a computer system, rendering it inaccessible to the legitimate users, has become a prevalent and increasingly sophisticated cyber threat [CSBS (2023)]. Following encryption, attackers demand a ransom payment, often in cryptocurrency, in exchange for providing a decryption key to restore access to the compromised data. The tactics employed by ransomware actors have evolved considerably over time. Initially, the primary goal was data encryption and ransom payment for recovery. However, a significant shift has occurred with the emergence of "double extortion" tactics [CSBS (2023)]. In these scenarios, attackers not only encrypt the victim's data but also exfiltrate sensitive information before encryption. They then leverage this stolen data, threatening to release it publicly if the ransom demands are not met. This dual approach significantly increases pressure on victim organizations to comply with ransom demands, as the potential consequences now include not only the loss of data availability but also the risk of sensitive data exposure.

Self-hosted payment systems, which are crucial for businesses to conduct transactions, face unique risks and challenges in the context of this evolving ransomware threat [Dispensa (2023)]. These systems are often directly connected to financial processing and handle highly sensitive information, including cardholder data [Dispensa (2023)]. This makes them particularly attractive targets for cybercriminals seeking financial gain through ransomware attacks. The compromise of a self-hosted payment system can lead to an immediate halt in payment processing capabilities, directly impacting an organization's revenue streams [Dispensa (2023)]. Furthermore, the sensitive nature of the data stored and processed by these systems means that a successful ransomware attack can easily escalate into a significant data breach, with severe consequences for the organization and its customers.

The potential impact of a successful ransomware attack on a self-hosted payment system can be far-reaching and devastating [IPC (2022)]. The most immediate consequence is often a significant loss of revenue due to being unable to process payments [Dispensa (2023)]. Beyond this, organizations face substantial costs associated with responding to the incident, including engaging forensic experts to investigate the breach, legal counsel to navigate data breach notification requirements, and specialized services to attempt data recovery [IPC (2022)]. In cases where personal or financial data is compromised, organizations may also incur legal fees and face regulatory fines due to non-compliance with data privacy laws [IPC (2022)].

The reputational damage resulting from a ransomware attack and subsequent data breach can be severe and long-lasting, leading to loss of customer trust and potentially impacting future business [IPC (2022)]. Moreover, ransomware attacks can sometimes lead to direct financial fraud, resulting in further monetary losses for the affected organization [IPC (2022)].

While cyber insurance policies can help offset some of these costs, obtaining and maintaining such coverage involves premiums and potential deductibles [IPC (2022)]. Downtime caused by ransomware can also lead to substantial financial losses due to disrupted operations and lost sales [Vanover (2023)].

2. Understanding ransomware tactics and techniques targeting payment systems

Ransomware attacks targeting self-hosted payment systems typically follow a predictable lifecycle, often beginning with gaining initial access to the network. Common attack vectors include phishing emails, which may contain malicious attachments or links designed to trick users into downloading malware or revealing credentials [PTP Cloud (2023)]. Exploiting vulnerabilities in exposed and poorly secured Remote Desktop Protocol (RDP) services is another frequently used method for initial intrusion [CISA (2025)]. Attackers also actively seek out and exploit known vulnerabilities in unpatched software and operating systems running on systems connected to the payment infrastructure [CISA (2025)].

Once attackers have successfully gained initial access to a system within the network, they often

engage in lateral movement [CISA (2025)]. This involves navigating through the network infrastructure to identify and compromise other systems, with the ultimate goal of reaching critical assets such as payment processing servers and databases [CISA (2025)]. Attackers utilize various tools and techniques to facilitate lateral movement, including leveraging compromised credentials obtained during the initial breach or through other means, and using protocols like RDP to remotely access other systems [CISA (2024)]. Privilege escalation is another common tactic employed during this phase, where attackers attempt to gain higher levels of access and control within the compromised systems and the network environment [CISA (2025)]. This allows them to perform actions that a standard user would not be authorized to do, such as disabling security controls or accessing sensitive data.

The core objective of a ransomware attack is to encrypt data, rendering the targeted payment systems and their associated data unusable [CSBS (2023)]. Many modern ransomware groups have adopted a "double extortion" strategy [PTP Cloud (2023)]. In addition to encrypting the data, they also exfiltrate sensitive information, such as cardholder data, before initiating the encryption process [PTP Cloud (2023)]. This stolen data is then used as additional leverage to coerce victims into paying the ransom, with the threat of public release if the demands are not met [PTP Cloud (2023)]. Given the highly sensitive nature of payment card information, preventing data exfiltration from these systems is of paramount importance [CISA (2023a)].

The act of data exfiltration itself constitutes a data breach, which carries significant legal and regulatory obligations for organizations, including mandatory reporting requirements in many jurisdictions [IPC (2022)]. Furthermore, ransomware attackers often target an organization's backup systems and recovery mechanisms [CISA (2025)]. By compromising or deleting backups, the attackers aim to eliminate the victim's ability to restore their systems and data without paying the ransom, thereby increasing the likelihood of payment.

3. Key vulnerabilities in self-hosted payment systems prone to ransomware attacks

Several key vulnerabilities commonly found in self-hosted payment systems make them susceptible to ransomware attacks. Insecure remote access configurations, particularly the exposure of RDP services with weak passwords or without the protection of multi-factor authentication (MFA), are frequently exploited by attackers to gain initial access to the network [CISA (2025)]. The use of weak or default credentials across various system components and applications also provides a simple yet effective entry point for malicious actors [CISA (2025)]. Inadequate access controls, where users are granted permissions beyond what is necessary for their roles, can further facilitate lateral movement and access to sensitive payment data once an attacker has compromised an initial account.

Outdated and unpatched software and operating systems represent another significant vulnerability [CISA (2025)]. Known vulnerabilities in these components are actively targeted by ransomware exploits, providing attackers with readily available pathways into the system.

Insufficient network segmentation and poorly configured firewall rules can also leave self-hosted payment systems exposed. A lack of network segmentation allows ransomware to spread rapidly from an initially compromised system to the critical payment processing environment, while inadequate firewall rules might permit unauthorized traffic to and from the payment system, creating opportunities for attackers [CISA (2025)].

The absence of robust backup and disaster recovery plans is a critical vulnerability that can significantly increase the impact of a ransomware attack [CSBS (2023)]. If backups are not performed regularly, stored offline in a secure manner, and thoroughly tested, organizations may find themselves unable to recover from a ransomware attack without resorting to paying the ransom. Finally, inadequate endpoint security measures, such as the lack of up-to-date antivirus and anti-malware software on servers and workstations that interact with the

1. A comprehensive overview of current ransomware mitigation techniques, including multi-layered defenses such as robust backups and employee training, is provided by Ojo (2025).

payment system, can allow ransomware to execute and spread within the environment [CISA (2025)].1

4. Comprehensive strategies for protecting self-hosted payment systems against ransomware

Protecting self-hosted payment systems from ransomware requires a comprehensive and proactive approach that encompasses multiple layers of security controls [Google Cloud (2023)]. Adopting a defense-in-depth strategy, which involves implementing a combination of technical, administrative, and physical safeguards at various levels, is crucial [IPC (2023)]. This ensures that if one security measure fails, others are in place to provide continued protection.

Establishing robust backup and recovery procedures is paramount [NCSC (2021). Organizations should regularly create offline backups of the entire payment system and all associated data, storing these backups in a physically separate location or an isolated cloud environment [NCSC (2021). Implementing immutable backups, which cannot be modified or deleted by ransomware, provides an additional layer of protection [Vanover (2023)]. Encrypting backups is also essential to safeguard against unauthorized access in the event that the backup storage itself is compromised [Cynet (2023)]. Crucially, the entire backup and recovery process should be regularly tested to ensure its effectiveness and reliability when needed [Vanover (2023)].

Implementing strong access controls and adhering to the principle of least privilege are fundamental

Table 1:
Recommended preventive measures against ransomware for self-hosted payment systems

Preventive measure	Description	Reference
Implement offline backups	Regularly create and store backups offline or in isolated environments.	11
Enforce MFA	Require multi-factor authentication for remote access and administrative accounts.	10
Regular patching	Establish a process for timely patching of operating systems, software, and firmware.	11
Network segmentation	Isolate the payment system within the network using firewalls and segmentation.	5
Endpoint security	Deploy and maintain up-to-date antivirus, anti-malware, and EDR solutions.	7
Security awareness training	Conduct regular training for personnel on phishing and social engineering risks.	10
Incident response plan	Develop and regularly test a ransomware-specific incident response plan.	10
Data encryption	Encrypt sensitive data at rest and in transit within the payment system environment.	6
Compliance adherence	Ensure compliance with relevant industry standards like PCI DSS and data privacy regulations.	9

Source: CSBS (2023)

security practices [Vanover (2023)]. Organizations should enforce strong password policies, including complexity requirements and regular password changes, and grant users only the minimum level of access necessary to perform their job functions [CISA (2025)]. Regular reviews and audits of user accounts and their associated access permissions are also necessary to identify and rectify any potential security gaps [NCSC (2021)].

Establishing a rigorous vulnerability management program is vital for proactively identifying and mitigating security weaknesses [PCI Security Standards (2018)]. This includes conducting regular vulnerability scans on all components of the payment system infrastructure. A timely patching process for operating systems, payment processing software, and all other applications must be implemented, with a priority placed on patching known exploited vulnerabilities [CISA (2025)].

Network security hardening measures are essential for protecting the payment system from unauthorized access. Implementing strong firewall rules to control both inbound and outbound network traffic is critical. Network segmentation should be implemented to isolate the payment system from other, potentially less secure, parts of the organization's infrastructure. Any unnecessary network services and ports should be disabled to reduce the attack surface. Hardening the Server Message Block (SMB) protocol can also help prevent lateral movement of ransomware within the network [CISA (2025)].

Enforcing multi-factor authentication (MFA) for all remote access points to the payment system and for all administrative accounts adds a significant layer of security. It is crucial to ensure that MFA is implemented using strong and reliable authentication methods. Deploying and maintaining up-to-date antivirus and anti-malware solutions on all servers and workstations that interact with the payment system is a fundamental security measure. Organizations should also consider implementing Endpoint Detection and Response (EDR) tools for more advanced threat detection and analysis capabilities [CISA (2025)]. Application whitelisting can further enhance endpoint security by restricting the execution of only authorized software [Google Cloud (2023)].

Conducting regular security awareness training for all personnel who have access to, or interact with, the payment system is essential for mitigating the risk of social engineering attacks like phishing [CISA (2025)]. Training should emphasize the importance of recognizing and reporting suspicious emails and other potentially malicious activities. Developing and regularly testing a comprehensive incident response plan specifically tailored for ransomware attacks targeting the payment system is crucial for ensuring a swift and effective response in the event of an incident [CISA (2025)]. This plan should clearly define roles, responsibilities, and step-by-step procedures for detection, containment, eradication, and recovery. Encrypting sensitive data both at rest and in transit within the payment system environment provides an additional layer of protection, safeguarding the confidentiality of data even if it is exfiltrated [CISA (2025)]. Finally, organizations handling payment card information must ensure compliance with all applicable industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS) [PCI Security Standards (2018)]. Staying informed about, and adhering to, relevant data privacy laws and regulations is also critical [IPC (2023)].

5. Responding to a ransomware incident affecting a self-hosted payment system

In the event that a ransomware attack successfully breaches preventative security measures, a well-defined and practiced incident response plan is critical for minimizing the impact and ensuring a swift recovery. The initial step upon suspecting a ransomware incident is detection and immediate isolation. All affected systems, including those hosting the payment system and any connected workstations or servers, should be promptly disconnected from the network to prevent the ransomware from spreading further. For payment systems hosted in cloud environments, taking snapshots of the affected volumes can be valuable for later forensic analysis [CISA (2025)].

Communication during this phase should ideally occur through out-of-band channels, such as phone calls, to avoid alerting the attackers that their presence has been detected [CISA (2025)].

The next phase involves containment and eradication. The specific ransomware strain involved should be identified to understand its behavior and

Table 2:
Key steps in responding to a ransomware incident affecting a self-hosted payment system

Incident response step	Description	Reference
Detection and initial response	Identify the attack, isolate affected systems from the network, and initiate communication.	5
Containment and eradication	Research the ransomware, terminate malicious processes, delete associated files, and secure the entry point.	5
Recovery and restoration	Restore the payment system and data from clean, offline backups, prioritizing critical systems. Do not pay the ransom.	11
Post-incident analysis and lessons learned	Determine the root cause of the attack, identify vulnerabilities, and update security policies and procedures.	11

Source: Google Cloud (2023)

potential removal methods. Any identified ransomware processes running on the affected systems should be terminated or disabled. All associated files and registry entries related to the ransomware should also be deleted from the compromised systems. It is crucial to identify the initial point of entry that allowed the ransomware to infect the system and to secure this vulnerability to prevent future reinfections [CISA (2025)].

Recovery and restoration are the subsequent critical steps. The payment system and its associated data should be restored from clean, offline backups. It is essential to prioritize the restoration of critical systems and functionalities first to minimize business disruption [CISA (2025)]. After restoration, the integrity and functionality of the recovered systems must be thoroughly verified [Vanover (2023)]. Under no circumstances should the ransom be paid to the attackers [CISA (2025)]. Paying the ransom does not guarantee data recovery and only serves to encourage future attacks.

The final stage of the incident response process is post-incident analysis and lessons learned. A detailed analysis should be conducted to determine the root cause of the attack and identify any security weaknesses that were exploited. Based on the findings of this analysis, security policies, procedures, and training programs should be updated to prevent similar incidents from occurring in the future [CISA (2025)].

6. The role of threat intelligence in protecting against ransomware

Threat intelligence plays a crucial role in bolstering an organization's defenses against ransomware attacks targeting self-hosted payment systems. By continuously monitoring threat intelligence sources, organizations can stay informed about emerging ransomware variants, the latest attack techniques, and indicators of compromise (IOCS) [Google Cloud (2023)]. This proactive awareness of the evolving threat landscape enables organizations to adapt their security strategies and remain ahead of potential attackers. Integrating threat intelligence feeds into existing security tools and processes can significantly enhance an organization's ability to identify and block known malicious actors and infrastructure [Google Cloud (2023)]. Leveraging threat intelligence resources provided by government agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) [CISA (2023b)], and national cybersecurity centers [NCSC (2021)] can provide valuable insights and actionable data to strengthen preventative and detective security controls.

7. Conclusion

The global financial ecosystem we operate in today is a rapidly changing landscape that is a very attractive target for attackers who are utilizing increasingly sophisticated techniques.

Protecting self-hosted payment systems against the persistent and evolving threat of ransomware requires a holistic and multi-layered security approach. Organizations must prioritize the implementation of robust preventive measures, including establishing reliable backup and recovery procedures, enforcing strong access controls and the principle of least privilege, maintaining a rigorous vulnerability management and patching program, hardening network security, enforcing multi-factor authentication, deploying comprehensive endpoint security measures, and conducting regular security awareness training for all personnel.

In the unfortunate event of a successful attack, having a well-defined and regularly tested incident response plan is crucial for ensuring a swift and effective containment, eradication, and recovery process. Furthermore, staying informed about the latest ransomware threats and tactics through continuous monitoring of threat intelligence sources is essential for adapting security strategies and proactively defending against emerging risks. By diligently implementing these recommendations, organizations can significantly enhance their resilience against ransomware attacks and safeguard their critical self-hosted payment infrastructure.

References

CISA, 2023, "Understanding ransomware threat actors: LockBit," Cybersecurity and Infrastructure Security Agency, June 14, https://tinyurl.com/mt4bbzsp

CISA, 2023b, "Stop ransomware guide," Cybersecurity and Infrastructure Security Agency, October 19, https://tinyurl.com/zh5ryvjw

CISA, 2024, "#StopRansomware: Blacksuit (Royal) Ransomware," Cybersecurity and Infrastructure Security Agency, August 27, https://tinyurl.com/ms8ubn84

CISA, 2025, "Stop ransomware guide," Cybersecurity and Infrastructure Security Agency, October 19, https://tinyurl.com/zh5ryvjw

CSBS, 2023, "Ransomware self-assessment tool 2.0 (R-SAT)," https://tinyurl.com/tdrf5w9k

Cynet, 2025, "6 ransomware protection strategies you must know," May 8, https://tinyurl.com/3bbkm99z

Dispensa, B., 2023, "Ransomware mitigation: top 5 protections and recovery preparation actions," AWS Security Blog, September 1, https://tinyurl.com/55pbn7su

Dopamu, O. M., 2024, "Cloud-based ransomware attack on US financial institutions: an in-depth analysis of tactics and counter measures," International Journal of Science and Research 13:2, 1872–1881

Google Cloud, 2023, "Best practices for mitigating ransomware attacks using Google Cloud,"

IPC, 2022, "How to protect against ransomware," Information and Privacy Commissioner of Ontario, October, https://tinyurl.com/4dwd5zxv

NCSC, 2021, "Mitigating malware and ransomware attacks," National Cyber Security Centre, September 9, https://tinyurl.com/3ttr783r

Ojo, A. O., 2025, "Ransomware trends and mitigation strategies: A comprehensive review," Global Journal of Engineering, Technology and Agriculture 22:3, 9-16

PCI, 2018, "PCI DSS Quick Reference Guide," PCI Security Standards Council, July, https://tinyurl.com/2nf3xdpd

PTP Cloud, 2023, "Protecting against ransomware," April, https://tinyurl.com/5crfzr8v

Vanover, R., 2023, "How to protect against ransomware: 6 best practices," Veeam, July 27, https://tinyurl.com/m5ysz7m

WE MAKE THINGS HAPPEN.

Leading change in Financial Services.

BELGIUM
UNITED KINGDOM
THE NETHERLANDS
FRANCE
GERMANY
SWITZERLAND

www.projectivegroup.com

Projective INSTITUTE