LogRhythm®
The Security Intelligence Company

Building on the right foundation:

Cybersecurity and building societies

LogRhythm
The Security Intelligence Company

Working smarter

Building societies have been integral to shaping the physical landscape by enabling members to become homeowners. These organisations remain an essential part of the communities they helped build. Building societies also inhabit another landscape – the financial services landscape, which due to their relatively small size, they do not control.

However, there are great opportunities for building societies to take advantage of what makes them special: their connection to their members[1]. Staying up-to-date with members' expectations and offering modern services, including access to digital products, will help building societies remain relevant. A strong reputation as a safe, sensible alternative to banks is a brand value that must be safeguarded. And in this age of growing cyberthreats, taking measures to better protect member information and keep it secure is a major part of this.

The lay of the land

Today's interconnected world offers great convenience for customers and a good opportunity for building societies to strengthen connections and deliver innovative products and services. However, in a world where cybercriminals launched 9.32 billion attacks globally in 2017, security is paramount[2].

A security breach is bad news for any business, but for a building society that needs a reputation as being trustworthy, stable, and secure, it can be extremely damaging. Even a message about a quick response to a breach and reassurances about customer data is a communication that is best avoided[3].

Keeping member data secure is paramount at a time when the ways in which organisations process personal information is under close review. Trust is critical for customers, and losing that trust means damaging business reputation.

In parallel, compliance with regulations and accounting standards is a challenge for building societies. This challenge grows as the volume of data increases and new regulations and standards are enforced. Under the General Data Protection Regulation (GDPR), data breaches must be reported within 72 hours, for example. Other bodies, such as the Financial Conduct Authority (FCA),

More than money:
The data held by a building society is as valuable as money to cybercriminals.

- Member financial information
- Member personal information and passwords
- Proprietary information, including financial projections, sales and marketing plans, and new product offerings

[1] Personal perspectives –opportunities for the building society sector
https://home.kpmg.com/content/dam/kpmg/pdf/2013/05/personal-perspectives-opportunities-in-building-society.pdf
[2] Over 9.32 bn malware attacks launched by hackers in 2017
https://teiss.co.uk/threats/9-32-bn-malware-attacks-launched-hackers-2017/?getcat=
[3] H&RBS Statement on cyber incident
https://www.hrbs.co.uk/14350-statement-on-cyber-incident/

LogRhythm
The Security Intelligence Company

Prudential Regulation Authority (PRA), and Payment Card Industry Security Standards Council (PCISSC) have additional requirements.

In addition to securing member information, building societies must also keep funds safe. Like banks, brokers and insurance companies, building societies hold and move large amounts of funds, making them prime targets for cybercriminals. Research by Accenture found that the average bank experienced 85 targeted cyberattacks per year. Of those attacks, one-third were successful[4]. With access to money on the line, cybercriminals are unlikely to care about the distinctions between building societies and banks.

Finally, even if building societies meet all of the compliance targets and they manage to keep cyberattackers out, they must protect against internal threats, whether it's embezzlement, theft of member data, or staff operating outside their authority.

Surveying options

The good news is that building societies can succeed at providing effective cybersecurity. Yorkshire Building Society proved this, winning Financial Services Team of the Year at the 2015 Cyber Security Awards[5]. With the right people, tools and processes, building societies can successfully manage the threats they face.

Intrusion detection, firewalls and antivirus tools form the first line of defence, but when someone penetrates that front line, building societies require a rapid detection and response. To manage threats effectively, they must first be identified. Whether the activity is from inside or outside the organisation, building societies need a clear, centralised view of network activity to detect unusual activity.

Good security information and event management (SIEM) can reduce the mean time to detect (MTTD) attacks, allowing for a rapid response. By employing user and entity behaviour analytics (UEBA), systems can learn normal patterns of user behaviour, flagging anomalous activity. Responses can even be automated, such as shutting down network access until the threat can be fully investigated. This reduces mean time to respond (MTTR), limiting the damage of an intruder or advanced attack.

They're coming for you: Distributed denial of service attacks and ransomware are two prevalent threats that can disrupt a building society.

- **Distributed denial of service (DDoS):** A DDoS attack seeks to overwhelm an online service by bombarding the servers with more information than they can handle, rendering them unavailable or even crashing them. This public disruption interrupts your business and inconveniences members. DDoS can be part of an attempt to penetrate and infect a network with ransomware or other malware. Audit legacy components for vulnerabilities and correct them or replace them.
- **Ransomware:** This malicious software encrypts the target's data. Attackers charge a ransom to unlock data. WannaCry is a well-known example. However, the particularly malicious 'wiper' NotPetya destroyed data even if targets paid the ransom in 2017.

[4] Building confidence: Solving banking's cybersecurity conundrum
https://www.accenture.com/t20170419T061542Z__w__/us-en/_acnmedia/PDF-44/Accenture-Building-Confidence-Solving-Banking-Cybersecurity-Conundrum.pdf
[5] Yorkshire Building Society wins cyber security award
https://business-reporter.co.uk/2015/07/20/yorkshire-building-society-wins-cyber-security-award/

LogRhythm
The Security Intelligence Company

Threats can take many forms. They can include ransomware, which are designed to infect systems and encrypt data until a ransom is paid, a mortgage officer transferring funds beyond his authority, or a branch manager copying member data before taking a job with a competitor. Detecting and shutting down these threats can save building societies money and reputation.

The clearer and more complete picture that proper network monitoring provides also makes meeting compliance goals faster and more straightforward. Additionally, a better view of the business can also reveal opportunities to improve processes and realise efficiencies.

Blueprint for success

LogRhythm can help building societies create a solid foundation for security and help meet their evolving needs. LogRhythm's NextGen SIEM Platform monitors the environment to detect malicious activity and enable a rapid response. Its embedded UEBA solution provides deep visibility into user activity, helping detect insider threats, compromised accounts, privileged account abuse and other user-based threats.

SmartResponse™ security automation, meanwhile, frees up time so in-house IT teams can focus on other important tasks and improve operational efficiency. Security teams can also receive additional support from the Analytics Co-Pilot Service which involves a LogRhythm expert supporting the team. This additional security resource helps customers understand threats and alarms, how to respond to security incidents and how to refine solutions.

The reports needed to verify activities and security for regulatory compliance and auditing requirements are supported by network and data monitoring. As a result, generating reports becomes less resource-intensive via automated, real-time processes. In addition, LogRhythm's centralised solutions for dedicated log management and security information and event management (SIEM) are designed for quick deployment and scalability.

Created for the payment card industry (PCI) environment, LogRhythm's solutions also provide visibility across networks and notify users immediately when suspicious activity is detected. These capabilities will help building societies meet the GDPR requirement to report any breach within 72 hours of it being discovered. The solutions also deliver additional information, such as remote access connection failures or missed scheduled software updates.

What LogRhythm brings to the job:
Success requires the right tools. Fortunately, LogRhythm has a full toolbox, enabling an organisation to build just the right solution for its needs.

- SIEM
- UEBA
- Real-time data management and network monitoring
- File integrity monitoring
- Security automation and orchestration
- User authentication, verification and monitoring
- Compliance
- Monitoring of privileged users with access to sensitive information
- Rapid detection, mitigation and auditing of threats
- Cloud security
- SmartResponse™ security automation
- Analytics Co-Pilot Service

LogRhythm
The Security Intelligence Company

Compliance demands are addressed by LogRhythm's Compliance Automation Suites with embedded content, while the platform enables long-term and secure data storage as well as wizard-based data recovery. Other capabilities include privileged user monitoring, web application defence, rapid forensics and advanced correlation and pattern recognition.

Another useful capability is LogRhythm CloudAI which takes data around document management systems and forwards it to the cloud, where it is subjected to machine learning across long periods of time to decipher patterns of behaviour and detect compromises. Alerts receive a risk score to help assess when something warrants attention.

Together, LogRhythm's offerings provide industry-leading automation, compliance and auditing support, comprehensive reporting, and protection against advanced threats. With the increasing need for building societies to have a reputation for keeping member data secure while offering modern services and meeting compliance requirements, these capabilities are essential. It pays to make the network as safe as houses.

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organisations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralising damaging cyberthreats. The LogRhythm platform combines user and entity behaviour analytics (UEBA), network traffic and behaviour analytics (NTBA) and security automation and orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations centre (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

"The visibility LogRhythm has given us has been a game changer. The insight we now have is unparalleled and gives us confidence that we can detect and mitigate a threat as soon as it appears."

– Donald Andango, Information Security Specialist, Salford Royal NHS Foundation Trust

LogRhythm®

The Security Intelligence Company

Security. Made Smarter.

Contact us

UK: **+44 (0)1628 918 330**
Germany: **+49 89 919292 - 200**
Middle East & North Africa: **+971 55 6422224**
europe@logrhythm.com | **www.logrhythm.com**