Saffron Building Society Proves Cyber Resilience for External Audits & Internal Governance with Cymulate

CASE STUDY

The Challenge

Saffron Building Society prides itself on delivering exceptional services, so maintaining a robust cyber security posture and ensuring business continuity is vital to the organization. The information security team, comprised of three in-house employees and two external contractors, is also responsible for Operational Resilience, which includes disaster recovery, business continuity management, crisis management, and cybersecurity incident response.

As a dual regulated financial services organization, Saffron Building Society is subject to regular internal and external audits. Additionally, its Executive Team has established internal governance processes to monitor the security team's cyber risk and provide monthly metrics alongside monthly and quarterly meetings with the broader security and risk teams.

To keep up with these audits and procedures, the small in-house security team needed a simple and accurate way to:

- **Prove cyber resilience**
  During its various audits, Saffron Building Society needs to provide assurance that it is assessing its cyber posture, managing its threats and vulnerabilities, and measuring its cyber risk. Each audit has different requirements.
- **Test against emergent threats**
  The team would receive information on new threats via threat feeds, but this did not provide immediate intel on whether the threat could be exploited in the organization's specific environment.
- **Continuously assess its security controls**
  Periodic penetration tests provided the team with a point-in-time snapshot of its security but were not an accurate and continuous evaluation of its security controls. Additionally, if the penetration test indicated that something needed to be remediated, a re-test would be required to determine whether its efforts to resolve the issue were successful thus incurring additional time and cost.

The security team identified a need for a security control and threat validation platform that would allow it to gain automated validation and data-based metrics on its daily performance.

The Cymulate Solution

Saffron Building Society decided to implement the Cymulate platform because of its ease of use, immediate threat assessments, data-based metrics, and excellent customer support.

Overview

Industry: Financial Services
HQ: United Kingdom
Size: 51-200 employees
InfoSec Team: 3 employees

"Cymulate gives us end-to-end visibility of our security posture, helps prove compliance, and saves my team a lot of time and effort."
- Adam Champion, Head of Information Security

Solution

- Breach and Attack Simulation
- Continuous Automated Red Teaming
- Attack Surface Management

Results

- Prove compliance requirements
- Increase team efficiency
- Continuously validate security

Adam Champion, Head of Information Security, explains that the team uses Cymulate to:

Prove compliance with financial regulators

"Cymulate allows us to easily present proof to external auditors of continuous control validation, threat assessments, remediation efforts, and general assurance that we effectively manage our cyber risk. Because each audit is different, we use different functions of the Cymulate platform to fulfill the various requirements. We can present ourselves as a very mature organization with an effective cyber strategy."

Assess against immediate threats

"Cymulate is an effective way to provide assurance to stakeholders about new and emerging threats being exploited in the wild. When a new threat emerges, the Cymulate Research Lab develops an immediate threats assessment so we can immediately test the threat against our security controls and quickly determine whether we are safe. Usually, by the time an Executive asks us if a particular new threat poses a risk to the Society, we have already run the Cymulate assessment and can provide the results."

Continuously validate security controls

"With Cymulate Breach and Attack Simulation, we continuously validate our controls to ensure they are working as expected. If we see any drift in a controls performance, we know where to focus our efforts. After following the platform's remediation guidance, we can immediately retest to validate that our efforts were effective."

Prioritize vulnerabilities

"Cymulate helps us evaluate whether a vulnerability is exploitable in our environment and enables us to prioritize remediation efforts. If there are compensating controls in place, we can prioritize remediating other high-risk vulnerabilities that are more likely to be exploited."

Increase cyber awareness among employees

"We use the Cymulate Continuous Automated Red Teaming phishing assessments to understand which of our employees might put us at risk of falling for a real phishing attack. It's important to have security controls in place, but it's also vital to reinforce good cyber habits with our staff."

Benefits

- **Proof of cyber resilience –** With Cymulate's metrics and dashboards, the security team can easily demonstrate that it is proactively managing its attack surface, validating its controls, and prioritizing high-risk security gaps.
- **Increased efficiency –** Cymulate helps the security team increase its efficiency, especially when validating against emergent threats. The team can react faster when an issue is identified and quickly provide assurance to the organization.
- **Depth and breadth of testing –** Cymulate's extensive library of threat intelligence-led risk assessments enable the security team to effortlessly test the different layers of each control, ensuring that the organization is not at risk.
- **Excellent customer and product support –** Saffron Building Society views its relationship with Cymulate as a partnership. Since implementation, the Cymulate customer success team has been available to assist and ensure the security team is optimizing its use of the platform.