CASE STUDY

# Global Bank Leader

Top 5 global bank reduced incident response time from 10 days to 5 hours.

The banking industry is charged with protecting the assets of businesses and consumers alike, and its members are well aware cyber criminals are continually looking for ways to access their systems.

Their chief security concerns are:

- The protection of monetary funds
- Personally identifiable information
- Intellectual property
- Business critical data

As cyber attacks continue to rise, the financial industry is on the forefront of the latest methods of detection, remediation, and resolution to threats on their systems.

According to the British Banking Association, 2013 heralded an exponential increase in cyber attacks.[1] The impact a breach has on a bank's reputation and client confidence is increasingly viewed as a critical risk. As the British Banking Association notes in its May 2014 Cyber Report, "If publicized, network security breaches can affect share prices, cause irreparable reputational damage and impact on the stability of the wider financial market." Unsurprisingly, the banking sector places a high priority on mitigating these risks. Last year, more than £700million was invested in cybersecurity in the UK alone.

In addition to bolstering its technological defense systems, the banking community shares information about the latest cyber attack methodologies including specific information on hacks, breaches, phishing websites and known criminals targeting them. A lot of this intelligence comes via the British Banking Association and various government incentives including the CBEST[2] vulnerability testing framework, launched by the Bank of England in June 2014, and the British Banking Association's Financial Crime Alert Service which provides real-time cybercrime intelligence from the National Crime Agency, the government and partner agencies.

"Banks have technology ceilings when it comes to email collections...We had a requirement for a potential solution for indexing and querying Microsoft Exchange data on the fly."

*Team member at top five global bank*

Financial services organizations across the globe are also increasingly participating in Services Information Sharing and Analysis Centres (ISACs). They are becoming a global go-to resource for cyber and physical threat intelligence analysis and sharing. The information includes analysis and recommended solutions from leading industry experts. The Financial Services ISAC[3] is currently active with members and partners.

[1] British Banking Association "The Cyber Threat to Banking," https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf

[2] Bank of England launches CBEST, June 2014 http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

[3] Financial Times, "JP Morgan data breach triggers calls for deeper collaboration," 3rd October 2014 http://www.ft.com/cms/s/0/7897ef22-4b1b-11e4-8a0e-00144feab7de.html#axzz3FCW0XFrI

across countries and regions throughout North and South America, Europe, the Middle East and Asia/Pacific. The FS-ISAC is unique in that it was created by and for members and operates as a member-owned non-for-profit entity.

## Challenge

One of the UK's top banks recently reviewed its security technology to assist it in combatting new cyber threats.

The company's director of forensics and eDiscovery explained that a variety of security tools are employed by the bank as part of its depth defense strategy. These tools are designed to prevent external attackers from getting into their systems. They also monitor internal systems for data attempting exfiltration, whether as a result of compromised systems, a malicious insider, or employees falling prey to social engineering.

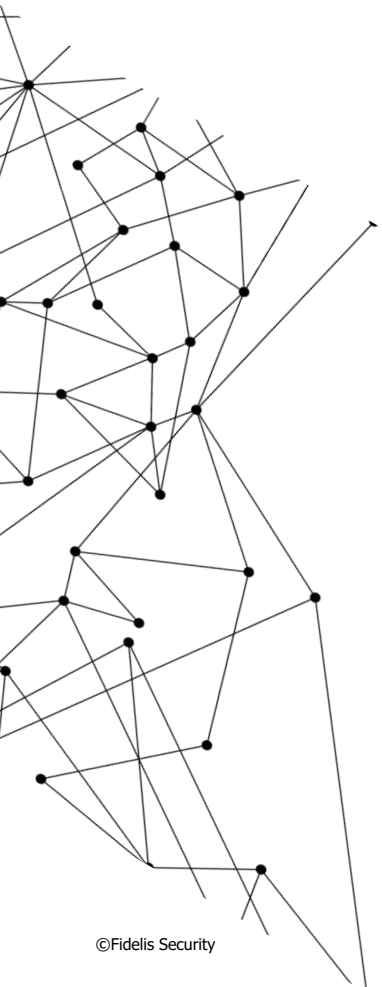
"While aspects of data protection are heavily regulated, some information is also considered sensitive to meet the bank's own business requirement to maintain confidentiality," he said.

One of the ways that this risk is mitigated is through the monitoring of email and internet traffic. However, the bank was limited in the volume of traffic that it could process.

"Banks have technology ceilings when it comes to email collections," explained a second team member, the company's global head of computer forensic investigations. "We had a requirement for a potential solution for indexing and querying Microsoft Exchange data on the fly."

"By having the Fidelis team embedded, they worked to quickly address hurdles at the proof of concept stage and delivered what the bank needed. We were looking for a proactive partnership."

*Head of Computer Forensic Investigations at top five global bank*





"Where previously you had to recover laptops and issue new ones; Fidelis Endpoint™ allows remote remediation on-the-fly. There's a given savings from not having to swap and replace hardware."

*Head of Computer Forensic Investigations at top five global bank*

## Solution

The bank sent out an RFI (Request for Information) to 40 forensics vendors including IBM, Symantec, Guidance, UIX, EMC2 (RSA), Fidelis Security and Standard Query.
A scoring index was used to narrow the final round of vendors to three. Based on its analysis, the bank selected Fidelis Security for cyber incident response.

Explaining the selection process, the company's director of forensics and eDiscovery stated, "Each vendor's product was assessed. It had to be compatible with Excel and it had to be compliant with financial industry regulations. Fidelis was the only security vendor that provided the indexing needed to query Exchange data on the fly."

## Results

As part of its security and cyber incident resolution strategy, the bank required an extension of the Fidelis endpoint analysis capabilities. The security team asked Fidelis for a roadmap feature that would automatically recover forensic material from endpoints impacted by malware.

"When the bank makes a major purchase, it's a partnership. We work with the selected vendor to develop the tools that we need. During the final selection we brought each of the vendors in, because we wanted their software engineers to meet our own internal software engineers," reported the company's director of forensics and eDiscovery.

"By having the Fidelis team embedded, they worked to quickly address hurdles at the proof of concept stage and delivered what the bank needed. We were looking for a proactive partnership."

He added that the endpoint agent was initially introduced for remediation of malware infections and used to restore laptops and desktops and recover malware for diagnosis and threat intelligence.

"Fidelis Endpoint™ had the capability to not only identify malware, but to restore endpoints to a known good point, kill malicious processes and recover malware, so that to some extent you could perform diagnostics."

The company's global director of director of forensics and eDiscovery explained that by working in partnership with the bank Fidelis developed additional capabilities to identify cyber incidents as they are unfolding. This allows the bank to perform incident resolution without having physical access to infected endpoints and has delivered an immediate cost saving to the bank.

"Where previously you had to recover laptops and issue new ones; Fidelis Endpoint allows remote remediation on-the-fly. There's a given savings from not having to swap and replace hardware," he added.

"On average, there is a cost of between $450 to $680 per desktop or laptop replaced, and in a bank there are many hundreds, so there's a real saving in cost."

Users of Fidelis Endpoint include the bank's incident response team, forensics team, data leakage team and intelligence team. He predicts that the firewall/IDS team is also likely to adopt it.



## Benefits

The bank's team also reported the forensic feature set of Fidelis Endpoint was easy for their staff to learn because many of the bank's incident response team are former police officers who are familiar "other forensic tools."

A major benefit of introducing Fidelis Endpoint is that the bank is now able to manage its own incident response in-house. This has enabled the bank to dramatically improve its cyber incident response times (Mean Time to Resolution) from ten days to five hours.

"An additional benefit of Fidelis Endpoint is that forensic teams have the same toolset as the incident response team who are reacting to any malware outbreak, so it provides a skill set and ease of use. We have a tool that can be used on the same platform, so the incident response team working on a malware outbreak can convert it into a forensic investigation at the same time," enthused the company's director of forensics and eDiscovery.

Another key benefit cited by the bank is the reduction of time and travel costs associated with each incident owing to the remote remediation and resolution enabled by the solution.

"For every incident, the fact that our team members don't have to fly to Singapore to help address it saves the bank £10,000," said the company's director of forensics and eDiscovery. "This is a nice value add, a bonus, but what we are more interested in is swiftness to respond and the avoidance of damage to our reputation."

## Incident Response Reduced from 10 Days to 5 Hours

The company's director of forensics and eDiscovery explained that certain regulatory bodies demand that banks report an incident within a matter of hours. Depending on an incident's severity, remediation must be completed within six to twenty four hours. He stated that a major benefit of introducing Fidelis Endpoint is that the bank is now able to manage

its own incident response in-house. This has enabled the bank to dramatically improve its cyber incident response times (Mean Time to Resolution,[4] MTR) from ten days to five hours.

"I think a better way of explaining the benefit is having an internal resource and software versus an external resource and software. If the bank ran an external forensics or incident response team, it generally takes external vendors about ten days from start to finish to do this as a project. You've got to identify the problem, raise a statement of work, raise a PO, bring investigators in on site, allow the investigators to undertake the retrieval, that normally involves traditional forensics work, where you go and image x number of hard drives, do the investigation and deliver the report. This takes about ten working days. The same response, using automated tools and trained incumbent staff, takes about four to five hours."

## Future Plans

In line with the British Banking Association's recommendations, the bank states that its key priority is intelligence sharing.

"When an event occurs, the system activates an alert. The incident response teams immediately react and remediate, or pass it to forensics. One of the key things we are looking at is asking other financial services entities and partners whether they've seen that type of attack before," stated the company's director of forensics and eDiscovery.

[4] Mean Time to Resolution (MTR) is the average time taken from initial detection of a cyber threat, through analysis and full remediation of the breach or attack. This measure is a key performance indicator of an organization's overall preparedness to handle cyber breaches and attacks.

While the bank regularly monitors for evolving classes of cyber attack, he explained that the majority of security issues are still tied to the inadvertent actions of insiders, such as clicking on malicious links in phishing emails. "Our current technology investment and sophisticated procedures allow us to detect the exfiltration of data as it is attempted."

The bank is also investigating investments in solutions for incident response on mobile devices as part of its BYOD security strategy. "We would be very keen to adopt an endpoint agent on mobile devices. However, BYOD data capture is difficult because of the legal issues surrounding privacy of data on personal devices," he stated.

He also reported that the next key step with Fidelis Endpoint is incident response that will assist the bank with compiling social media data and managing risks related to cloud-based application use. The company director also predicts that traditional computer forensics will be fundamentally changed by cloud computing.

"We took a collaborative approach when working with Fidelis and that has paid off. It's not about what they are selling — it's about what we require," said the company's global director of computer forensic investigations and eDiscovery concluded.