Case study

International financial services provider

Ethical hacking ensures customers can bank on online services from a global financial institution

Few companies attract as much online criminal attention as banks. The prospect of accessing confidential financial information is a powerful lure for hackers, and any security breach can have severe consequences for brands and bottom lines.

The wholesale division of one global financial services provider deals with the threat by getting BT Global Services to probe its defences and uncover vulnerabilities before criminals can find them.

BT has been doing the job for a decade. In that time, it's found weaknesses that could have significantly compromised the bank ... and it's always got there before anyone else, making sure customers enjoy secure banking at all times.

"It's like an insurance policy. No bank would like to see its name in the newspapers in relation to a security problem."

Global Security Officer, International Financial Services Provider

BT

Case study

International financial services provider

> "BT has found significant issues prior to go-live, which would have been grave if they had been present in live applications. The security tests really proved their value in mitigating potential security issues."
>
> **Global Security Officer, International Financial Services Provider**

BT Assure ethical hacking services instil confidence and security in global financial institution's online services

Staggering size of cyber threats to financial services

Banks have been favoured targets for criminals since the days of the Wild West. But today's felons are less likely to blow doors off safes and more inclined to put virtual barriers to the test. Cyber criminals can compromise a bank's online defences with complete anonymity from anywhere in the world. And many do.

While much of the concern focuses on retail activities, the threat is just as important for wholesale where banks provide services like currency conversion and large trade transactions for major corporate customers. Because the sums involved are so large, no wholesale banking provider can afford a security breach. Apart from direct financial loss, a serious hack could lead to irreparable reputational damage. But with cyber criminals constantly testing defences, what can banks do to avoid break-ins?

Of course, while this case study focuses on the security posture of just one bank, and while the financial services sector arguably stands to lose the most, the danger is clear and present across all industries.

As stated in the Ovum Decision Matrix: Selecting a Global Telco Managed Security Services Provider report[1] "There is increasing demand for managed security services, and we expect further growth in demand from enterprise customers frustrated with the increasing cost and complexity of securing IT and networks. Enterprise customers need help with responding to new threats, managing multiple security solutions, and analysing disparate security information that still keeps them open to breaches."

The assurance of ethical hacking

One international financial services provider has approached the problem by getting BT Assure to beat hackers at their own game. It retains a BT team to probe defences, uncover vulnerabilities and spot security gaps. BT is essentially paid to hack into the bank's systems ... before a criminal can.

BT is one of just four companies accredited to provide STAR (Simulated Targeted Attack and Response) services by CREST, a not-for-profit professional services regulatory organization serving the technical information security marketplace.

With the international bank, BT Assure ethical hacking services are applied to any new online product or service. They also get used whenever the bank's online properties, such as its corporate web site, go through an update or major change.

Currency transfer services, online money ordering, mandates and more, all get thoroughly checked before going live. In many countries, BT Assure also tests the bank's retail banking services. When the team finds a problem, it describes the risk, rates the severity of the issue and suggests remedial action.

Compelling evidence over the entire systems landscape

Sometimes the problem's not even in one of the bank's systems. BT also tests standard industry applications used internally in the bank. It's not uncommon to find faults in anything from core banking software to HR systems.

The test results can provide compelling evidence. In one case a BT ethical hacker was able to crack the security of a commercial employee benefits system and change the value of someone's discretionary bonus payment from €2 to €500,000. In these cases, the bank notifies the supplier of the fault. Sometimes BT has ended up advising the supplier as well as the bank on such vulnerability issues.

Whether problems are located in the bank's own systems or third party systems, tracking them down is critical. "BT has found significant issues prior to go-live, which would have been grave if they had been present in live applications," says the bank's global security officer. "The security tests really proved their value in mitigating potential security issues."

Since new vulnerabilities appear all the time, the BT team has a busy testing schedule. It carries out between 50 and 100 tests a year, not just on new code but also with existing software on a regular basis.

BT

[1] Ovum Decision Matrix: Selecting a Global Telco Managed Security Services Provider (TE007-000800) 17 Sep 2014 Available at: www.globalservices.bt.com/uk/en/solutions_category/create_a_secure_organisation?cid=(pl)btcom(cm)furl(lk)btassure_securitythatmatters

Case study

International financial services provider

"Everything that goes from BT Assure to the internal test teams is clear enough for the technical guys to start fixing straightaway. BT is our top supplier and applies a rigorous review process to test reports; not always the case with other providers."

Global Security Officer, International Financial Services Provider

Versatile and evolving BT Assure team

The size of the core team varies between a couple of people and around half-a-dozen, depending on workload. The BT Assure experts come with ethical hacking skills not only previously acquired and honed on the job, but also through security certification training and attendance at black-hat conferences.

Typical vulnerabilities tracked include cross-site scripting, which enables attackers to inject client-side scripts into web pages viewed by other users, and SQL injection, which is used to attack data-driven applications. "These are issues that in an online banking situation are potentially very dangerous," says the global security officer.

The bank uses a range of IT security providers and changes them on a regular basis to make sure there are no blind spots. But the BT service has been a mainstay of its security portfolio for the best part of a decade. BT Assure ethical hacking is offered as a recommended security option for software and systems development teams as part of a comprehensive security approach. "The BT team has shown it's actively following the latest cyber threats and testing has changed accordingly," says the global security officer. "They're on top of things."

Rigorous reviews and operational risk mitigation

Throughout the time BT has been providing the service, the bank has never suffered a significant security breach. But it could have: at one point, for example, the BT team showed how it could bring down the bank's web site through a distributed denial-of-service attack. Standard web protection systems had not detected the threat.

Besides the vulnerabilities that get spotted in time, one of the metrics the bank keeps an eye on is the level of BT report escalations. "Everything that goes from BT Assure to the internal test teams is clear enough for the technical guys to start fixing straightaway," says the global security officer. "That's key in the performance of an external security testing team. As long as it gets delivered, I only see reports saying what's been found and what's been fixed. BT is our top supplier and applies a rigorous review process to test reports; not always the case with other providers."

Comprehensive security testing isn't just important in safeguarding the bank's reputation, but also in complying with regulations like Basel III. The fact that BT provides the service helps ensure stringent operational risk standards are being met.

Global reach with a flexible resourcing model

Another advantage of working with a provider like BT, with global reach, is that the bank can call on local resources to help with projects in specific territories. Similarly, the central BT Assure team, spread across Europe, can be augmented with experts from around the world as and when the situation demands it.

The global security officer says: "BT has an expert team available at all times. They may have to deliver bad news but they always act very professionally, putting lots of passion and extra hours in. For example, finding a zero-day vulnerability on Friday afternoon and fixing it by Saturday morning. We've never hit the news because of a hack. A key reason for that is strict security testing and BT is part of that."

Core services

- BT Assure ethical hacking

BT

Offices worldwide

Registered office: Grand Canal Plaza, Upper Grand Canal Street, Dublin 4
Phone +353 (0)1 4325000 Freephone 1800 924 924
Registered in Ireland No. 141524

Find out more about BT Ireland

www.btireland.com

Freephone 1800 924 929

business@btireland.com