Factsheet

security against cyber threats for financial institutions and their customers

Online theft and fraud is now a business: a fast-growing, successful, increasingly professional business.

The cyber security challenge

The past decade has seen an exponential rise in the number of online and now mobile transactions. Smart retailers have built entirely new business models on this phenomenon, to the point where online and mobile service providers are handling billions in financial enquiries, purchases and money transfers each year.

Criminals can spot these trends, become expert in emerging technologies and use them all to their own advantage. No business with an online, mobile or multi-channel presence is safe from being targeted by criminals, and the most tempting targets of all are banks. As the institutions that store and distribute funds, that provide loans and handle transaction processing for the world, banks are potentially very vulnerable: the Mandiant M-Trends Report 2014 shows that Financial Institutions are now the subject for 15% of all cyber-attacks. Most significantly, that is an increase of 40% in just one year, (between 2012 and 2013).

The same trends can be seen in phishing: the method most commonly used to steal customer identities for online fraud. Today, the main threat is not an armed robber but a cyber-intruder, identity fraudster or professional gang that works systematically to break down their online defenses.

A growing range of cyber-threats

Cyber-crime is a global business, with criminal enterprises that mirror normal businesses in their working practices. They have a worldwide reach, they fund technology research, recruit talented graduates and provide benefits and incentive schemes. In other words, this is not just about one or two individuals looking for easy opportunities: it is real industry, and it grows stronger each year.

Yet external threats are not the only factor in driving the need for a reliable cyber-security policy. We operate in a marketplace that increasingly depends on flexible collaboration and rapid, Omni-Channel transactions. There is exponential growth in financial transactions from mobile devices, in particular, and that leads to growing concern about data security as more and more information is exchanged across mobile and collaborative networks.

With individuals increasingly working on the move or from remote locations, the integrity of communication networks becomes more important all the time. And, of course, the potential dangers caused by employees being careless, or bearing a grudge against their own company, or of systems that stay active after employees have moved on mean that internal threats are growing as well. As businesses become more fast-moving and agile, so more and more potential gaps start to open up in their defences against cyber-crime.

Financial institutions need to take the right action to close those gaps, compete successfully against criminals and keep their customers safe in an environment that is becoming increasingly unsafe.

Financial Institutions are now the subject for 15% of all cyber-attacks. Most significantly, that is an increase of 40% in just one year, (between 2012 and 2013).

The risk and security environment

Financial institutions today operate in an environment in which risk is not just a primary concern but also a multi-dimensional and highly complex issue.

They need to consider a number of strategic risk parameters, many of which are directly connected to regulatory requirements. This makes it necessary not simply to safeguard information and transactions against cyber threats but to be highly proactive in developing methods, processes and technologies, driven by an end-to-end, top-to-bottom strategic vision for always keeping one step ahead.

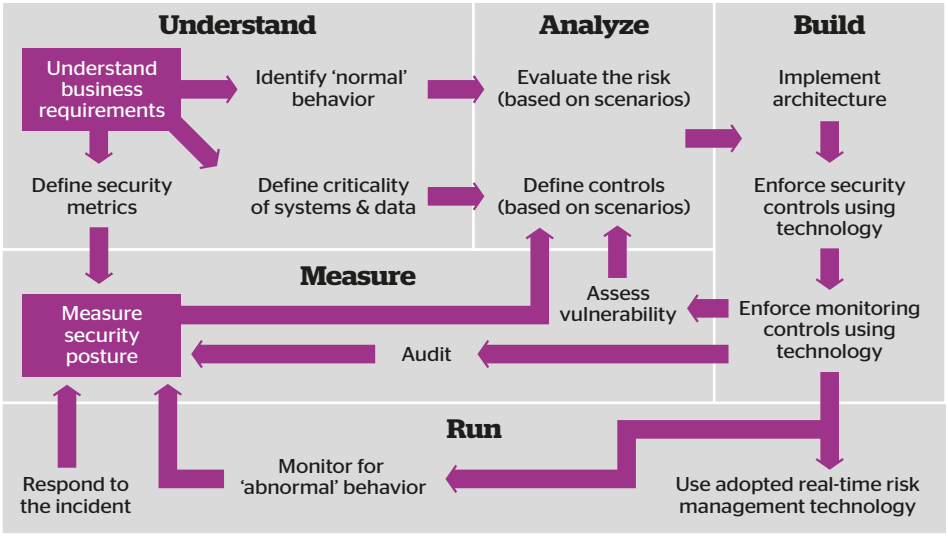
Security covers all connections to and interactions with customers, employees (which now includes ecosystem partners) and all forms of counter-party, and this category could include participants in a trade, partners in a value chain and members of a wider community, consortium or interest group. This is a highly dynamic landscape, and the enemy of real security in this space is fragmentation. Financial institutions have effective security methods in most individual areas but Atos believes that even the most capable banks do not necessarily have a comprehensive and all-round view of both existing and emerging threats.

Until a truly strategic security solution is in place, they cannot assume that they, their customers and partners or their brands are safe. Many financial institutions are routinely subjected to Denial of Service attacks, both by conventional criminals and politically motivated hacktivists. The results can be devastating, with customer records being lost and reputational damage caused in ways that leave a lasting impact.

Five principles and processes for effective cyber-security

In this complex, unpredictable commercial and social landscape, Atos has identified five key principles that are central to building effective security, illustrated opposite.

- **Understand:** define business requirements and priorities, establish what is normal
- **Analyze:** evaluate risk and define controls
- **Build:** create security architecture and enforce controls
- **Measure:** assess vulnerability and enforce monitoring controls
- **Run:** measure for abnormal behavior and respond to incidents fast.



As a world leader in all aspects of integrated security, Atos knows from long-term, hands-on experience how to ensure that principles are turned into effective processes and solutions, keeping financial institutions and their customers safe in an uncertain world.

To build the highest level of cyber-security protection inside any financial institution and its ecosystem, the process we follow, for the five principles is simple:

Vast numbers of customer records leak into the public domain each year. In 2012 and 2013: 46,000 customer records from a major insurance company; 175,000 merchant records from a payment systems company; 40 million credit card accounts from a card payment processing company were leaked, all resulting in large fines and serious damage to reputation.

Understand	▶ Identify priority processes ▶ Identify information within key processes that must be kept safe ▶ Establish clear policies to define the context for security procedures.
Analyze	▶ Define technology solutions that will safeguard information and processes ▶ Locate areas of potential vulnerability within the company and its ecosystem.
Build	Build cyber-capabilities targeted at: ▶ Infiltrators from the outside (cyber defense) ▶ Collaborators in the ecosystem (cyber collaboration) ▶ Careless or disaffected insiders (cyber identification).
Measure	▶ Establish proven and effective monitoring tools and methods ▶ Enforce policies through monitoring and challenge failures ▶ Audit performance and continuously review to identify emerging areas of vulnerability.
Run	Implement trusted cyber operations, covering: ▶ Organizing, covering the entire workforce and external partners ▶ Enabling, covering data in transit, access and information settings ▶ Anticipating, preventing attackers from entering and removing them fast if they do ▶ Preparing, to strengthen readiness and maintain operations.

Successful cyber-security operations will always use this approach, creating a trusted framework for safeguarding an organization and its customers in an increasingly insecure world.

A world class cyber-security model

Cyber threats are evolving all the time, and that means solutions must develop fast and efficiently.

Atos cyber-security solutions are based on a proven model for integrated security that protects a complete organization against all credible threats, from outside and in. The Atos model begins with policy-making and behavior and includes specific solutions designed to counter a range of individual threats.

The cyber-security landscape covering a large enterprise and its ecosystem

Atos addresses the seven key dimensions of cyber-security in the above comprehensive framework:

1. **Cyber risk management.** Putting in place a comprehensive policy that covers effective Business Continuity Management and enterprise-wide Governance.
2. **Cyber security advisory.** Integrating every element that relates to security processes within a complete security architecture, with full integration of IT and Operational Technology, ensuring that sensor information is also managed and protected.
3. **Cyber operations.** Keeping the entire IT environment secure, based on a Security Operation Center (SOC) and incident and event management.
4. **Insider threat protection.** Effective methods for ensuring that data is not lost as a result of internal attacks, routine migration or any other factor.
5. **Secure cooperation.** Bringing the additional level of physical security that only integrated encryption technologies can offer, including biometrics, Public Key Infrastructure or use of cards and tokens.
6. **Digital identity & access control.** From outside and within an organization, the greatest danger often comes from unauthorized access. Atos solutions deal with this critical issue through Identity and Access Management (IAM), Role and Compliance Management and building Federated Identity for secure single sign-in.
7. **Cyber intelligence.** Security analytics to identify issues and threats from outside or inside in real-time, managing all areas of vulnerability and conducting forensic responses to any incidents.

Atos builds on deep, long-term experience of providing security solutions to organizations that require uncompromising protection, and we have used these skills and capabilities to build a complete, proven approach to addressing the risks of financial institutions today.

Atos Security, Risk and Compliance solutions help banks and insurance companies to:

- **Deal with the growing threats from organized crime**
- **Manage the potential for fraud caused by greater collaborative working**
- **Safeguard business from insider threats**
- **Maintain full compliance with constantly-changing regulations**
- **Build trust with customers, regulators and partners alike.**

Atos cyber-security in action

In financial institutions across Europe and beyond, Atos know-how, expertise and solutions are bringing enhanced security for organizations and their customers.

Leading global bank

For one of the world's largest and most prestigious retail and investment banking groups, headquartered in Europe, Atos is a long-term strategic partner. For operations across the world, Atos systems, solutions and people are engaged in delivering security monitoring, Endpoint Security, email encryption and secure mobile platform, keeping the business and reputation of the bank safe.

A world-leading reinsurance company

Headquartered in Switzerland, this is one of the most trusted and successful insurers. For operations in 20 countries, they use an Atos solution, to ensure foolproof identity management, with a single consistent method used in all corporate offices, remote locations and on the move. This leads not only to enhanced security performance but greater productivity and simplicity for the business.

Global leading provider of ratings, benchmarks and analytics in the global capital and commodity markets

Atos has played a key role as strategic IT partner in helping this long-established, world-famous U.S. based company, strengthen its status as a key provider of information to financial institutions and customers alike. Atos provides security architecture, service provision, design and execution as part of a major outsourcing contract that covers 44 countries and 20,000 employees.

The ultimate security story: the Olympics

Atos has been the IT partner of the International Olympics Committee (IOC) since 1992 and, following a recent contract extension, will remain the key security provider to the IOC up to 2026. The Olympics is the single most complex event on Earth for volume of communication traffic, multi-organization working and targeting by cyber-criminals. All of the challenges faced by financial institutions are all encountered at the Olympics – but on a larger scale.

For the IOC, Atos builds a tailor-made cyber framework, using the principles outlined earlier, and uses this to deal with millions of alerts (255 million in London 2012) and identify real threats in order to neutralize them. The lessons learned at the Olympics are analyzed and used to strengthen and enrich Atos cyber security solutions for other markets, including financial services.

IOC President Thomas Bach said:
"Technology is critical to the success of each edition of the Olympic Games. We are delighted that we will be able to continue relying on Atos and its vast experience to deliver flawless, innovative IT services."

Why Atos?

Atos is a proven leader in all areas of cyber-security, based on more than 30 years continuous service with armed forces, security agencies, emergency services and other organizations that do not and cannot accept anything less than a near perfect operational security record. In addition, Atos brings world-class intellectual property to the security field, with leadership positions in encryption, IAM, biometrics and Managed Security Services.

Most important, Atos knows financial services from the inside. We work for 7 out of the 10 largest European banks and for 6 out of the 10 largest insurance companies in the world. As industry insiders, we understand the key trends, developments and transformational changes taking place across the financial world. Atos understands the need to match improved customer experiences, greater speed, agility and responsiveness with an uncompromising approach to security. That is what we deliver.

For more information, contact: dialogue@atos.net