High performance. Delivered.
By the very nature of their business, investment banks possess vast quantities of highly sensitive information, ranging from the portfolios and transaction histories of wealthy individuals to the details of pending mergers. When such information is compromised—whether by determined cyber criminals or individuals within the organization by accident—the consequences, in terms of reputational damage and monetary losses, could be significant.

Traditionally, investment banks have always been highly aware of the importance of safeguarding customer and transaction data and have taken all the steps deemed necessary to do so. In the current environment, however—with organized cyber criminals running industrialized hacking operations and freely selling and/or sharing information about institutional vulnerabilities—investment banks may be dealing with forces that cannot be addressed exclusively by internal resources.

In this environment, cyber security becomes not only a major challenge for investment banks, but also a key responsibility of their boards of directors and senior management teams. Boards and management need to consider:

- The organizational structure and reporting arrangements for cyber security operations.
- The experience and expertise of the chief information security officer (CISO), and the need to balance industry knowledge against “street smarts” as they pertain to cyber issues.
- Safeguarding data in a networked environment, which may encompass cloud data storage and the provision of services via the cloud.
- Creating a culture that is both security-conscious and aware of the financial and reputational consequences of data breaches.
Firms that displayed leadership in cyber security shared certain characteristics, including immediate reporting of security incidents to the CEO and board of directors, clear definition of responsibility and authority pertaining to security, and effective communication of security requirements to all employees.

As they migrate their operations from custom-built IT systems to flexible, cloud-based platforms integrated into a digital ecosystem, investment banks need to address these and other cyber security concerns with comprehensive, well-thought-out solutions. With data housed outside of the traditional confines of a private data center, cloud security becomes a responsibility shared with service providers and internal security resources. It is worth noting, however, that cloud security problems are solvable, assuming appropriate governance and organizational structures are in place.

For investment banks, securing digital platforms should begin before development work starts. Investment banks can reduce risk by collaborating with potential partners to identify possible security challenges across and beyond their industry. They should also identify what types of security-related data the platform can gather and ways that cyber security operations can be leveraged to monitor edge and core devices for abnormal activity.

A pervasive concern

Cyber security is a widespread and pressing concern for most executives. As Figure 1 shows, a worldwide survey of over 900 executives conducted by Accenture Strategy found that over two-thirds of respondents believe the likelihood of a cyber attack to be “very” or “extremely” high (and a similar share sees a high likelihood of data or privacy breaches). But only nine percent run inward-directed attacks and intentional failures to test their systems on a regular basis. There is a significant disconnect between cyber threat awareness and preparedness in most organizations.

Addressing structural issues

For investment banks, effective cyber security begins at the top with the board of directors and senior management. Firms need a structure that recognizes the business issues connected to cyber security, while providing the expertise needed to deal with specific and ever-changing threats. Security models and tools are proliferating, creating complexity and potentially compromising security, so an integrated approach is needed to make the best use of new solutions.

<table>
<thead>
<tr>
<th>Defending the digital investment bank</th>
<th>Source: Accenture Research</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable business growth and secure operations</td>
<td>Addressing boardroom and C-Suite concerns about the effect of security breaches on shareholder value, revenue and compliance</td>
</tr>
<tr>
<td>Reinventing security to be “digital friendly” by supporting user centricty and Internet scale, and addressing digital concerns such as big data, Internet of things and commerce</td>
<td>Gaining security-situational awareness across expanding business boundaries and developing a rapid-response capability</td>
</tr>
<tr>
<td>Developing solutions to manage technology and process security risks outside of direct organizational control while leveraging security “as a service”</td>
<td>Testing environmental robustness and implementing security automation to offset staff shortages</td>
</tr>
</tbody>
</table>

Figure 1: Cyber threat awareness and preparedness

<table>
<thead>
<tr>
<th>Active Testing</th>
<th>Likelihood of Attack</th>
<th>Privacy Breaches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only 9% proactively run inward-directed attacks and intentional failures to test their systems on a regular basis</td>
<td>67% believe the likelihood of an attack is “very” or “extremely” high</td>
<td>68% believe there is a high likelihood of privacy breaches of personal data</td>
</tr>
</tbody>
</table>

Source: Accenture Research
A 2015 study conducted by Accenture and Ponemon Group found that firms that displayed leadership in cyber security shared certain characteristics, including immediate reporting of security incidents to the CEO and board of directors, clear definition of responsibility and authority pertaining to security, and effective communication of security requirements to all employees.\(^1\) At leading companies, the CISO is more likely to report directly to a senior executive, set the security mission by defining strategy and initiatives, and have a direct channel to the CEO in the event of a serious security incident. They also provide sufficient resources for cyber security teams to deal with existing threats, while researching and preparing for new types of attacks.

**Securing the edge**

New technologies—particularly those in the area of mobile communications—are opening new horizons for investment banks and their clients. Transactions are no longer limited to landline telephones or desktop computers; mobile phones and tablets now serve as effective platforms for many activities. However, the functionality of such devices has often outpaced the ability of investment banks and other financial services firms to protect customers’ privacy and prevent unauthorized access to their accounts.

Investment banks that provide secure mobile applications could differentiate themselves, but few have the technological sophistication to do so today. Innovation often takes place at the tactical level, without the benefit of a high-level, holistic view of security concerns. Investment banks, like other financial services firms, need to find a balance between maintaining security and providing an optimal customer experience.

**Adopting new technologies**

Some players have begun exploring promising new technologies to identify and prevent cyber incursions. Following in the footsteps of retail banks that are using biometric authentication at automated teller machines in certain countries, some investment banks are piloting voice biometrics for added security and a better customer experience during telephone transactions. Others are exploring new authentication methods, such as social log-ins and risk- or content-based identification. Although still in very early stages, such services may soon represent a competitive advantage for firms with tech-savvy clients.

Investment banks can benefit from important features of new security technologies, including the ability to identify anomalies in network traffic, prioritize threats and provide advance warnings of possible breaches. Whether business is conducted on an in-house legacy platform or through the cloud, investment banks should regularly evaluate their vulnerabilities. They can apply threat monitoring to understand potential problems and leverage threat intelligence to understand when cyber criminals (or rogue individuals within the organization) are attempting to take advantage of such vulnerabilities. In some cases, data visualization may help identify problematic behavior—not only by cyber criminals, but also by customers, counterparties and employees.
The “big-picture” approach

For investment banks, the need to bring technology to market quickly to maintain a competitive advantage—along with the ever-evolving sophistication and boldness of cyber criminals—has left cyber security struggling to catch up. Investment banks can benefit from applying several “big-picture” principles to cyber security. In addition to a “top-down” view starting with the board and senior management, these include:

• A proactive stance. Accenture’s research and experience suggests that investment banks should take a proactive approach toward cyber security, continually monitoring, testing and experimenting with new technologies. Reactive cyber defense is no longer sufficient to maintain an effective security program and regulatory compliance.

• A broad view of risk management. Cyber risk should be considered alongside traditional enterprise risks to more effectively inform risk management decision making. In the Accenture 2015 Global Risk Management Study, nearly two-thirds (65 percent) of financial services executives surveyed said that cyber and IT risk would have an increased impact on their business in the next two years and that they are making talent and organizational decisions accordingly.1 Demand for cyber security skills is escalating quickly.

• A willingness to collaborate. Investment banks’ internal cyber security teams may have been capable of dealing with yesterday’s threats. In the current environment, however, investment banks will need not only outside expertise, but also effective collaboration with cloud and other service providers to deal with emerging threats. Investment banks may also need to increase their willingness to share information regarding such threats with governments and industry groups, including the Financial Services Information Sharing and Analysis Center (FS-ISAC).

• Attention to the “human factor.” Many breaches occur as a result of human error, negligence or failure to follow security protocols. Privileged access management is a top risk in this area. Investment banks should have organized and integrated programs to raise awareness of security issues, encourage proper procedures and assign responsibility when individuals are at fault. Insider threat networks should be enhanced and user behavioral analytics should be deployed to manage the human components, whether malicious or accidental.

Cyber security will remain a major challenge for investment banks for the foreseeable future. By adopting an active cyber security strategy, a sound organizational structure, effective training and communications, and new technology, investment banks can begin to address their cyber security concerns and devote more resources to growth-oriented activities over time.

Five Security Recommendations to Stretch Your Boundaries in the Digital Era

01. Enable secure, autonomous devices at the edge.

As edge devices such as sensors and smart meters increase and become more autonomous, security should encompass the potential risks to those devices, such as physical tampering, data integrity and unauthorized access. Understand and proactively address the security implications of decisions being made at the edge. Manage and safeguard edge devices and the end-to-end technologies that enable intelligent decisions.

02. Make data-driven decisions at Internet of Things (IoT) scale.

Increasingly larger amounts of data are collected, processed and analyzed by organizations. Establish end-to-end security on data. Develop and maintain a data assurance program as the center of your IoT strategy. Build a data assurance program that directly ties to the business model and enables more informed decisions based on accurate data.

03. Secure volume, variety and velocity of big data.

The exponential growth of big data is straining traditional database management systems. In moving to big-data platforms, apply the principles of information security across all aspects of data collection and management. Take a data-centric security approach to address the volume, acquisition velocity and data variety being collected for the organization.

04. Maximize protection across digital ecosystem platforms.

Digital industry and cross-industry ecosystems and platforms are developing to support the IoT. Combine operational and security information across the enterprise—and across platforms—to help businesses respond effectively to the rapidly changing cyber landscape. Work with ecosystem partners to brainstorm security challenges and develop responses.

05. Build customer trust in a digital economy.

Successful digital enterprises will establish and maintain customer trust based on how they collect and protect their data. Be vigilant with security and privacy practices so as to not compromise customers’ experiences or lose their trust. Follow proactive and ethical data stewardship practices and offer enhanced services that are consistent with customers’ expectations of privacy and personalized, seamless experiences.


Source: Accenture Research
About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 358,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is www.accenture.com.

Contact Us

To discuss any of the ideas presented in this paper, please contact:

Charlie Jacco
Florham Park
charles.a.jacco@accenture.com

Timothy Elliott
Detroit
timothy.c.elliott@accenture.com

Disclaimer

This report has been prepared by and is distributed by Accenture. This document is for information purposes. No part of this document may be reproduced in any manner without the written permission of Accenture. While we take precautions to ensure that the source and the information we base our judgments on is reliable, we do not represent that this information is accurate or complete and it should not be relied upon as such. It is provided with the understanding that Accenture is not acting in a fiduciary capacity. Opinions expressed herein are subject to change without notice.