8 Steps to Modernize Security for the Application Economy

ca technologies

8 Steps to Modernize Security for the Application Economy

Executive Summary

Today's application economy of tech-savvy end users, with their increased demand for apps and services across an explosion in Internet-connected devices, is forcing IT and business leaders to substantially re-invent their approach to IT security. In short, security must evolve from its "limit and protect" foundation to an "unleash and empower" future.

Security needs to enable access not only for internal end users, but also external customers and partners. The focus shifts from an approach of limited access with extensive restrictions to a strategy that uses enabling technologies–such as open application programming interfaces (APIs), two-factor authentication and bring-your-own-identity—to enable new business innovation and opportunities.

Recent research shows executives understand this fundamental shift in thinking about IT security and recognize the need to update their approach. Vanson Bourne conducted a survey of 1,425 senior IT and business leaders, including 142 Chief Security Officers and Chief Information Security Officers. The CA-sponsored survey revealed:

- Security is considered a top obstacle to success in competing in the application economy.
- Preventing data breaches is the top security priority, followed by improving the mobile customer experience.
- Mobility is significantly impacting how IT and business leaders approach security.
- Nearly four-fifths of respondents enable access to APIs for customers, partners or suppliers.
- One quarter of all IT spending will be devoted to security three years from now.

The study also sheds light on the significant change in thinking toward security as a business enabler versus a control mechanism. Nearly half of all respondents (47%) now acknowledge that security is either entirely or mostly

about enabling the business, or it must work in balance with control. As a result, 78% have already seen or expect to see increased revenue from new services enabled by improved security.

The final in a series of five reports exploring the impact of the application economy (all available on rewrite.ca.com), this research report examines what your peers are doing to more effectively leverage security as a business enabler and highlight eight steps you can take now to modernize your security approach.

The Application Economy is Shifting Security Priorities Toward the Customer Experience.

The application economy increases opportunities for businesses to expand products and services via technologies such as mobile, but it also increases the threat landscape significantly with hyper-connected end users, numerous Internet-enabled devices and diligent hackers looking to do harm on both small and large scales.

This promise is coupled with greater risk, making security one of the most significant success factors for IT and business leaders. Survey respondents identified security as the top obstacle to becoming more effective in the application economy. The right security approach can empower the business; the wrong one will limit innovation and hinder success in today's economic environment and put the business at risk.

The study results show that IT and business leaders already understand that security today goes beyond putting controls in place, to providing customers with the experience they expect with apps and mobility (See Figure 1).
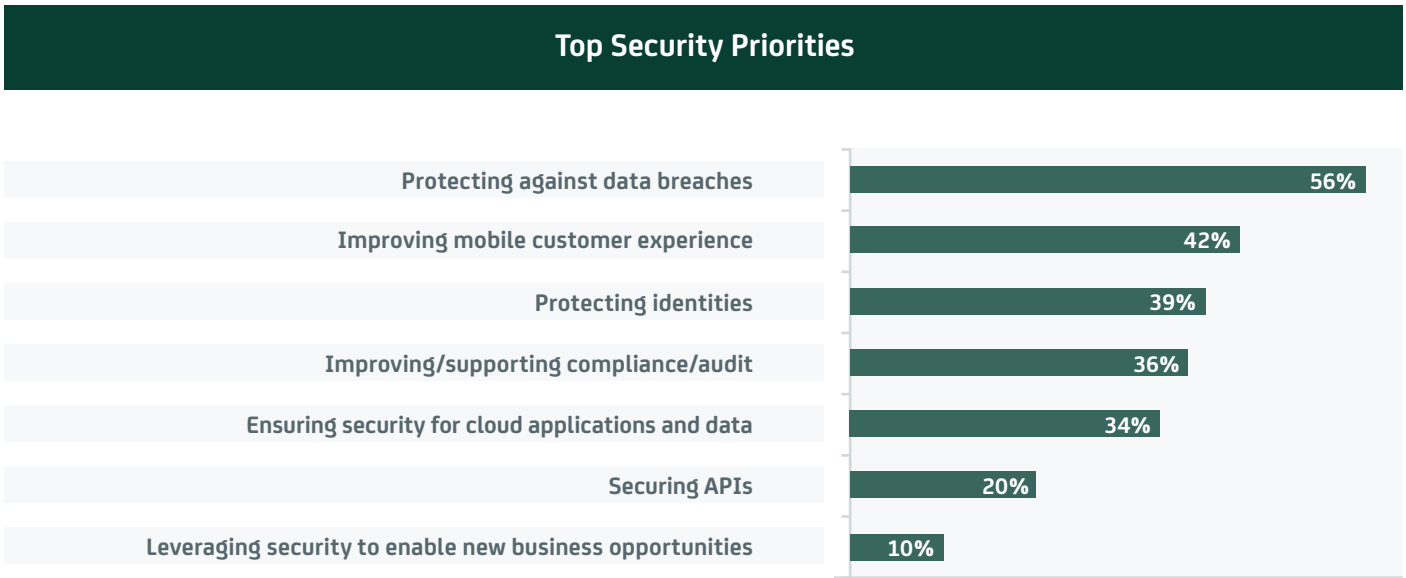
Top Security Priorities

Protecting against data breaches	56%
Improving mobile customer experience	42%
Protecting identities	39%
Improving/supporting compliance/audit	36%
Ensuring security for cloud applications and data	34%
Securing APIs	20%
Leveraging security to enable new business opportunities	10%

Figure 1.
Which of the following do you consider to be the most important security priorities in your organization? (Select three.) Total: 1,425

Protecting against data breaches topped the list for more than half (56%) of respondents, which makes perfect sense because security will always be about protection. But new priorities are coming to the forefront for security. Significantly, improving the mobile experience is considered a top three security priority for 42% of those polled here, ahead of protecting identities. IT and business leaders realize their job is to make the customer happy, on all fronts. If mobile apps are what the customers want, IT security must learn how to deliver them securely.

Why IT Security Must Evolve From Control to Enable

IT and business leaders must deliver more apps and services than ever before, and with this increased demand for enhanced access comes the critical need to securely enable innovation and growth.

Enabling end users, customers and partners to do business freely is becoming as important as protecting against threats for a growing number of IT and business leaders (See Figure 2).
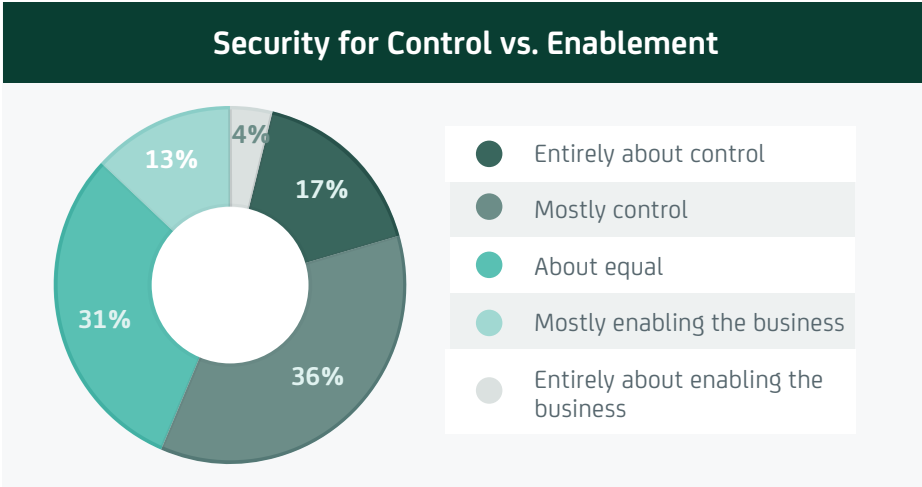
Security for Control vs. Enablement

●	Entirely about control
●	Mostly control
●	About equal
●	Mostly enabling the business
●	Entirely about enabling the business

Figure 2.
Is security mostly about control (protecting data or apps) or is it about enabling the business? Total: 1,425

In fact, security for control and security for enablement should not be mutually exclusive. This study shows that the slight majority of those favoring control over enablement share some of the same priorities with the growing number of enablers (See Figure 3).

Top Security Priorities: Enablers vs. Controllers

	Enablers	Controllers
Protecting against data breaches	56%	55%
Improving mobile customer experience	42%	44%
Protecting identities	39%	38%
Improving/supporting compliance/audit	24%	44%
Ensuring security for cloud applications and data	42%	30%
Securing APIs	23%	22%
Leveraging security to enable new business opportunities	14%	8%

Figure 3.
Which of the following do you consider to be the most important security priorities in your organization?
Total 236 Enablers and 754 Controllers

On more than a few key points, enablers and controllers see security priorities similarly. Enablers favor technologies that can drive business growth, such as mobility, cloud and APIs, but also acknowledge the heightened need to protect against data breaches in the application economy. Yet controllers don't consider security for cloud applications and data as important as enablers do.

The largest disparity in point of view between enablers and controllers can been seen in their responses to priorities around improving/supporting compliance/audit. Forty-four percent of controllers find this a priority, while just 24% of enablers consider this among the most important security priorities.

Another difference in apparent in respondents' responses on the priority of leveraging security to enable new business opportunities. Fourteen percent of enablers see this as a priority, whereas only 8% of controllers recognize this need. Enablers see existing and emerging technologies as opportunities, and they see security as contributing to the success of these technology endeavors.

Opening APIs and Securing Mobile Apps Enable the Business to Innovate.

Both mobility and technologies such as APIs—which can enable more secure interactions among multiple parties—require more thought be put into security. How businesses are dealing with the demand for mobility and employing APIs for integrations with partners or suppliers indicates how well they are putting security to work for them.

For instance, nearly 80% of IT respondents to this survey are opening access to their APIs externally for suppliers, customers and partners (see Figure 4). APIs can be used to launch innovation services or provide new channels for distribution. They can be used in mobile apps, cloud platforms and to address emerging requirements in the Internet of Things. But APIs could also be exploited by hackers, so strong security is essential when exposing APIs to third-party developers and others.
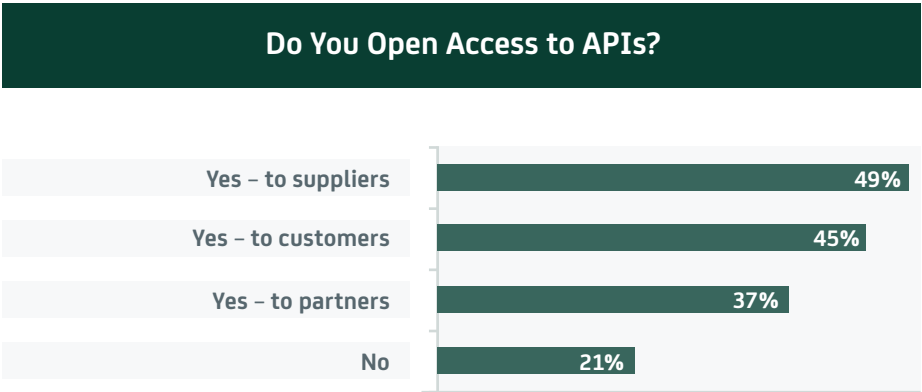
Do You Open Access to APIs?

Yes – to suppliers	49%
Yes – to customers	45%
Yes – to partners	37%
No	21%

Figure 4.

Do you open up access to your APIs to customers, suppliers or partners? Total: 714 IT Respondents Only

As more companies explore the benefits of APIs and examine how to mitigate the risk of opening APIs, a significant number of survey respondents are also considering how mobility is impacting their security policies and practices. Nearly half (49%) of all respondents report seeing a significant/big impact of mobility on their security practices and policies for employees or customers (See Figure 5).
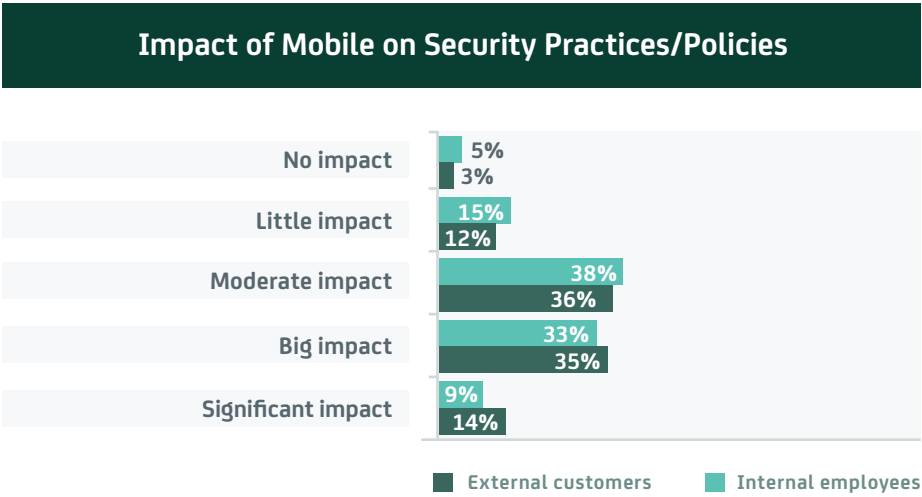
Impact of Mobile on Security Practices/Policies

	Internal employees	External customers
No impact	5%	3%
Little impact	15%	12%
Moderate impact	38%	36%
Big impact	33%	35%
Significant impact	9%	14%

■ External customers   ■ Internal employees

Figure 5.

To what extent are mobile apps/devices impacting your security practices/policies for your employees or customers? Total: 1,425

The demand for mobile access from employees expecting enterprise apps to be as user-friendly as their favorite consumer-focused apps has caused IT departments to expand the breadth of their coverage to employee-owned devices. Now the increased and persistent demand to create mobile apps and services so that customers can more easily interface with the business is adding to the impact mobility has on security.

Investing in Security and Reaping the Rewards

Technology, business demand and customer experience are all driving IT and business leaders to increase the focus on advanced security in the application economy. The increased focus will be evident in more budget dollars being devoted to security, according to the results of this survey (See Figure 6).
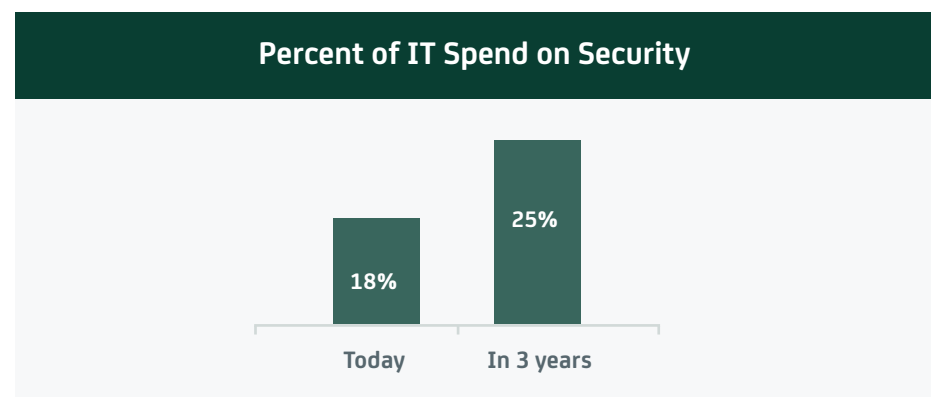
Percent of IT Spend on Security

18% Today

25% In 3 years

Figure 6.
What percentage of your organization's IT budget is being spent on security now and will be spent in three years? Total: 714 IT Respondents Only

With IT leaders expecting to spend one-fourth (25%) of their entire IT budget on security in three years, up from 18% today, they also expect to reap security rewards from the bigger investments. Staying true to the broad range of requirements in the application economy, the anticipated benefits of enhanced security range from fewer security breaches to increased revenue.

Nearly all (94%) of the study's respondents have already seen or expect to see fewer security breaches. This is significant, because a business lives or dies by its brand. A security breach can not only put company data such as employee or customer information at risk, but it can also create a publicity nightmare as word spreads quickly across multiple social networks. Almost 90% of those surveyed also have or want to have more accountability and control from increased security.

From there, the results shift from traditional security concerns to today's more business-enabling security focus. For instance, 87% have already experienced or anticipate experiencing improved customer satisfaction and trust in their products and services. Another 86% have seen or expect to see an increase in the number of customers using the business' apps or services. And the expected benefits go on to include more business-focused results, such as increased user productivity, business flexibility and revenue growth from new services enabled by improved security (See Figure 7).
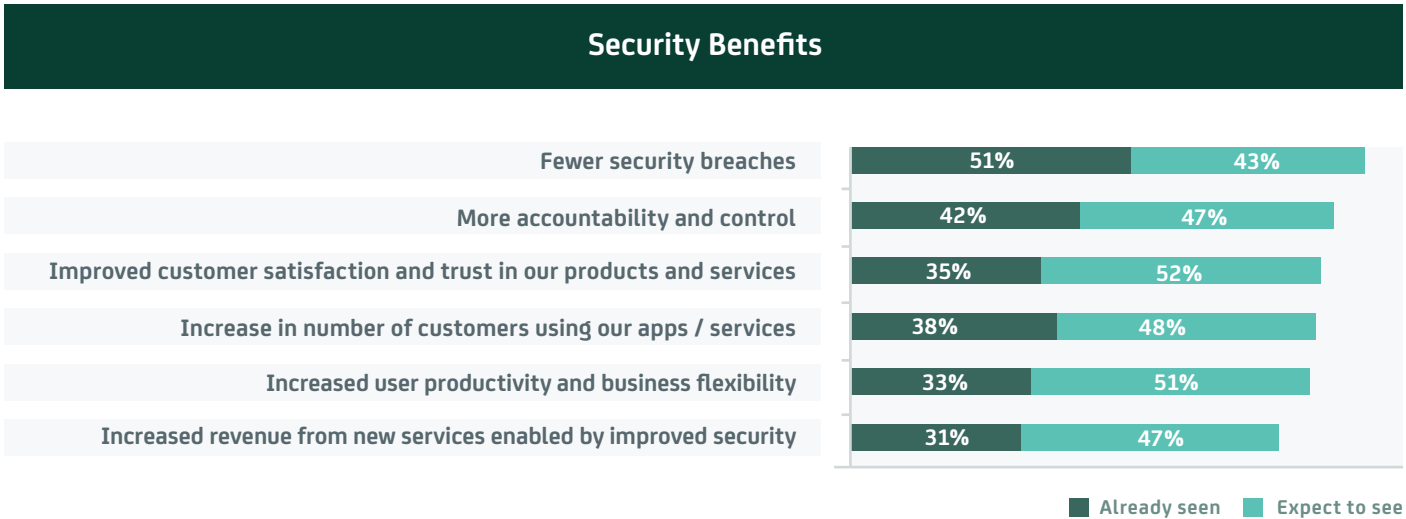
Security Benefits

	Already seen	Expect to see
Fewer security breaches	51%	43%
More accountability and control	42%	47%
Improved customer satisfaction and trust in our products and services	35%	52%
Increase in number of customers using our apps / services	38%	48%
Increased user productivity and business flexibility	33%	51%
Increased revenue from new services enabled by improved security	31%	47%

■ Already seen ■ Expect to see

Figure 7.
What benefits have you seen or would you anticipate seeing from improved security in your organization? Total: 1,425

Measuring the benefits of increased security among the organizations already experiencing positive results shows that the payoff is tangible for organizations investing more in security. The benefits with the most significant reported improvement are related to customer satisfaction and trust in products and services, and an increased number of customers using apps and services.

Overall these results reflect why security that enables business growth is critical: customer experience and revenue growth.

On the other hand, the top desired result of fewer security breaches also shows the least quantifiable improvement, proving the threat environment is more challenging in today's economic environment (See Figure 8).

Security Improvement Results	
Benefit/Metric	**Improvement**
Improved customer satisfaction and trust in our products and services	23%
Increased in number of customers using our apps/services	21%
More accountability and control	21%
Increased revenue from new services enabled by improved security	20%
Increased user productivity and business flexibility	19%
Fewer security breaches	17%

Figure 8.
What has been the percentage improvement, increase or reduction for each of the quantifiable benefits you have seen? Total: 652 who have already seen benefits and could quantify the benefits

How Application Economy Leaders Approach Security Differently

The transformation toward security as an enabler is already happening for leaders in the application economy.

For the purposes of this study, "leaders" and "laggards" were determined by CA Technologies and Vanson Bourne based on respondents' answers to three survey questions:

- Whether they think their organization is very/highly effective in managing the challenges of the application economy;
- The number of customer-facing applications developed in the past year; and
- Whether they had already acquired or have near-term plans to acquire a software company to gain needed expertise.

The study represents a distribution of 24% leaders, 16% laggards and 60% in the middle.

The survey finds that leaders approach security differently and get better results than their counterparts. To start, they spend more on security (See Figure 9).
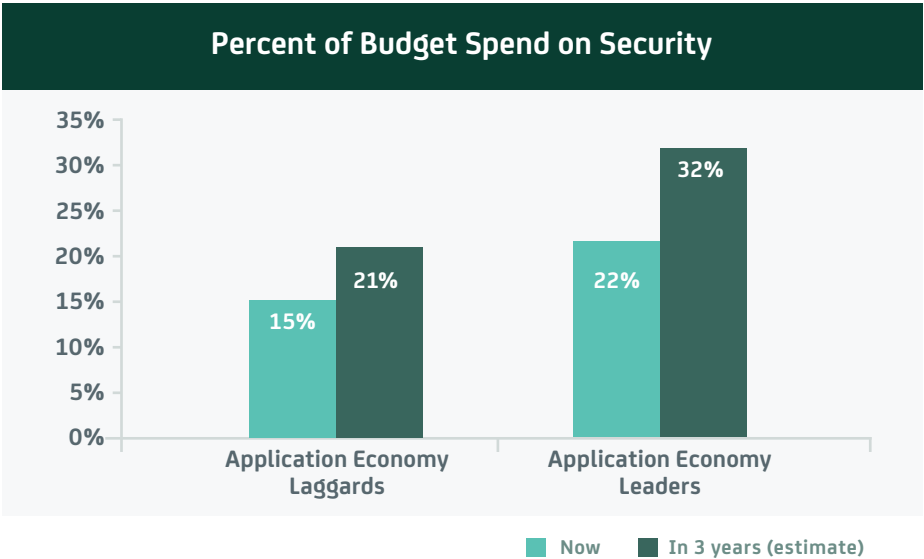
Percent of Budget Spend on Security

Figure 9.
What percentage of your organization's IT budget is being spent on security now and will be spent in three years? Total: IT respondents only, 116 Enablers and 379 Controllers

Leaders also acknowledge the importance of developing mobile apps and opening APIs for partners, suppliers and customers (See Figure 10 and Figure 11).
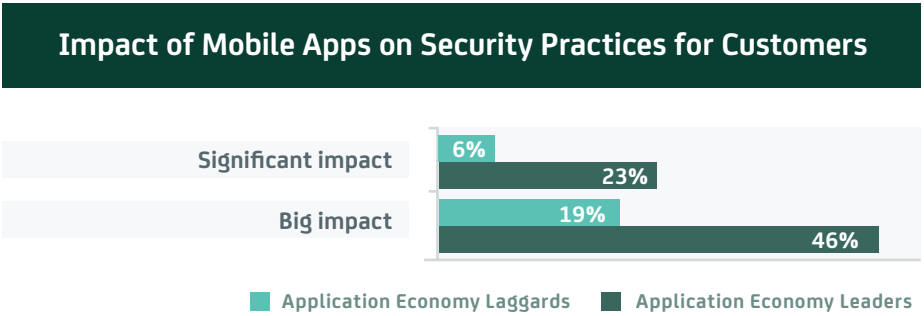
Impact of Mobile Apps on Security Practices for Customers

Significant impact — 6% / 23%
Big impact — 19% / 46%

Application Economy Laggards   Application Economy Leaders

Figure 10.
To what extent are mobile apps/devices impacting your security practices/policies for your customers? Total: 236 Enablers and 764 Controllers

API Access

Open Access to APIs — 59% / 93%
Don't Open Access to APIs — 41% / 7%

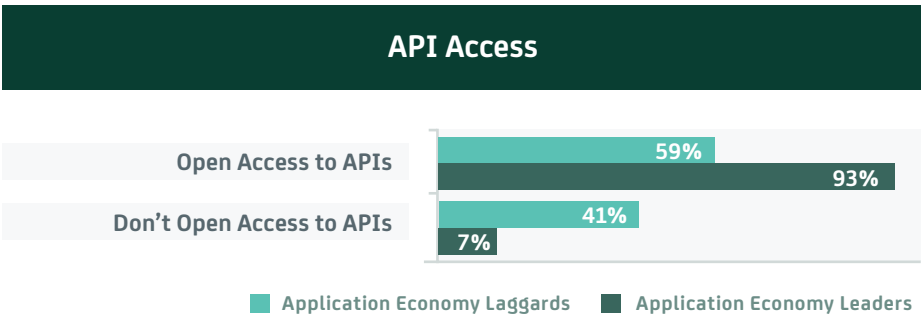Application Economy Laggards   Application Economy Leaders

Figure 11.
Do you open up access to your APIs to customers, suppliers or partners? Total: IT respondents only, 116 Enablers and 379 Controllers

Leaders investing more in security and addressing new technology demands are also experiencing more business benefits to enhanced security than their laggard counterparts (See Figure 12). The results experienced by leaders show security as a business enabler that will deliver the desired outcome in today's economic environment.
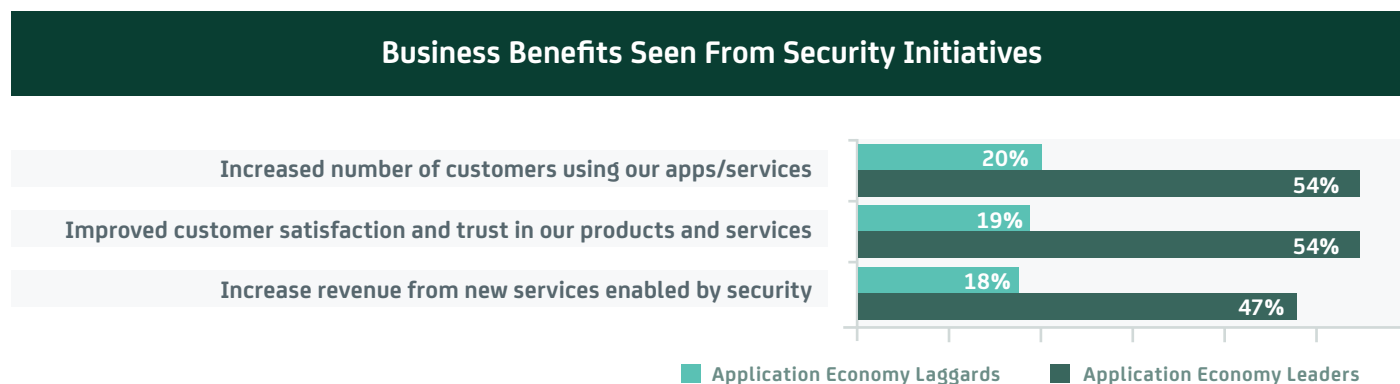
Business Benefits Seen From Security Initiatives

Increased number of customers using our apps/services — 20% / 54%

Improved customer satisfaction and trust in our products and services — 19% / 54%

Increase revenue from new services enabled by security — 18% / 47%

■ Application Economy Laggards   ■ Application Economy Leaders

Figure 12.
What benefits have you seen or would you anticipate seeing from improved security in your organization? Total: 236 Enablers and 764 Controllers

Eight Steps to Take Now to Modernize Security for the Application Economy

The data garnered from this survey shows clearly that security must evolve to meet the growing and changing demands in the application economy. Newer desired outcomes such as customer experience with mobile apps drive security priorities as much as traditional security results like fewer data breaches.

The savvy IT and business leaders will instruct their security specialists to find ways to provide access to the appropriate assets and resources while also protecting critical data. Here we share guidance on how to embrace secure enablement for the business:
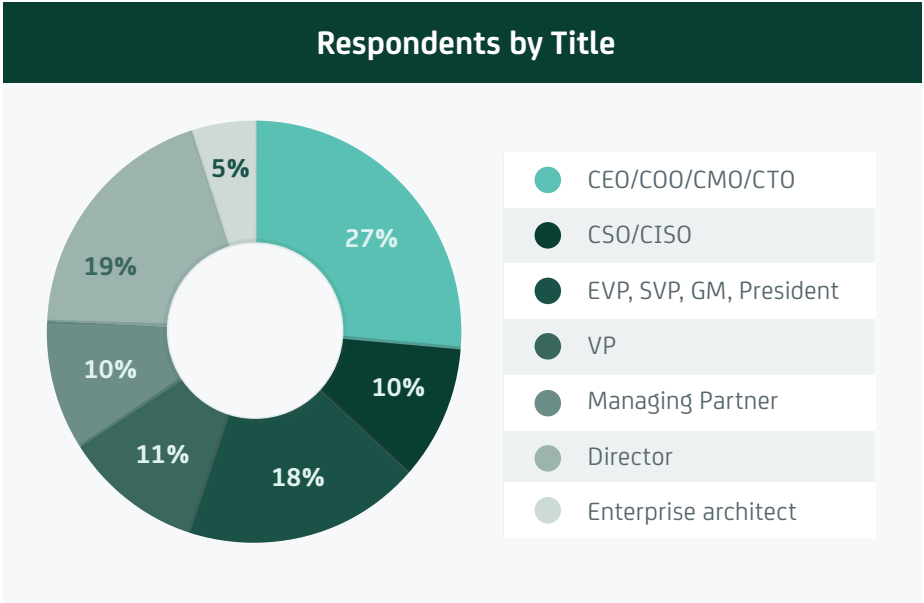
1. **Understand the customer experience and how it is impacted by security practices.** A seamless and frictionless customer experience is a desired outcome of security in the application economy. That means security professionals need to know how customers expect to interact with apps and their security policies.

2. **Bring security technologies to the innovation table.** Security technologies such as single sign-on, identity self-service, transparent risk modeling and secure APIs open new business opportunities for the business. CSOs and CISOs need to educate business leaders and software developers on how existing and emerging technologies can be applied

to drive business success. With this input, security will be viewed as an enabler, not a blocker.

3. **Bake security in from the beginning.** Encourage the security team to collaborate with developers at the beginning stages of creating new apps and services, and incorporate security into every IT program from the start.

4. **Invest in security by justifying business value.** As demand for new apps and services grows, IT and business leaders must allocate funds to expand their approach to security. Build this investment into the cost of new revenue-generating projects that enable business success. This survey shows investments in security can lead to improvements in customer experience and increases in business revenue.

5. **Assess your current approach to mobile security.** Your customers' use of mobility is evolving rapidly, and your security practices may not have kept pace. It may be time to assess how you can improve mobile security for employees, customers and partners.

6. **Open APIs and allow the business to innovate.** Proper use of APIs can open up your data securely—to your partners and developers. They help create an ecosystem of complementary services that can expand markets and open up new customers and opportunities. Security can prevent unauthorized access to APIs, monitor data usage, implement velocity controls and block hack attempts at the gateway while enabling the business to drive new business programs.

7. **Examine the threat landscape.** Protecting the apps and services required in the application economy also requires security experts to know the increased threats and risk made possible by mobility, cloud and the Internet of Things, for instance. But there are more and different threats; IT and business leaders, security professionals and end users all need to be educated on the new threat landscape.

8. **Strike a balance between control and access.** There is evidence that using security as a business enabler delivers the results businesses want to see. But that doesn't mean security can abandon its roots in protection and control. An appropriate balance of enablement and control is critical to support the needs of employees, partners and customers.

Methodology

This global study was conducted online by Vanson Bourne in July-August 2014 with 1,425 senior IT and line-of-business executives at enterprise organizations with revenues of at least US$500 million. Job profile of respondents:

Respondents by Title

- CEO/COO/CMO/CTO — 27%
- CSO/CISO — 10%
- EVP, SVP, GM, President — 18%
- VP — 11%
- Managing Partner — 10%
- Director — 19%
- Enterprise architect — 5%

The survey was conducted across five industry verticals of financial services, healthcare, retail, telecommunications, and media/entertainment in the following 13 countries: United States, Canada, Brazil, U.K., France, Germany, Italy, Switzerland, Spain, Australia, China, India and Japan.

For More Information

For further information on this research report as well as the latest news and research on the application economy, visit **ca.com/rewrite**.

About CA Technologies

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact, and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

ca technologies

Connect with CA Technologies at ca.com