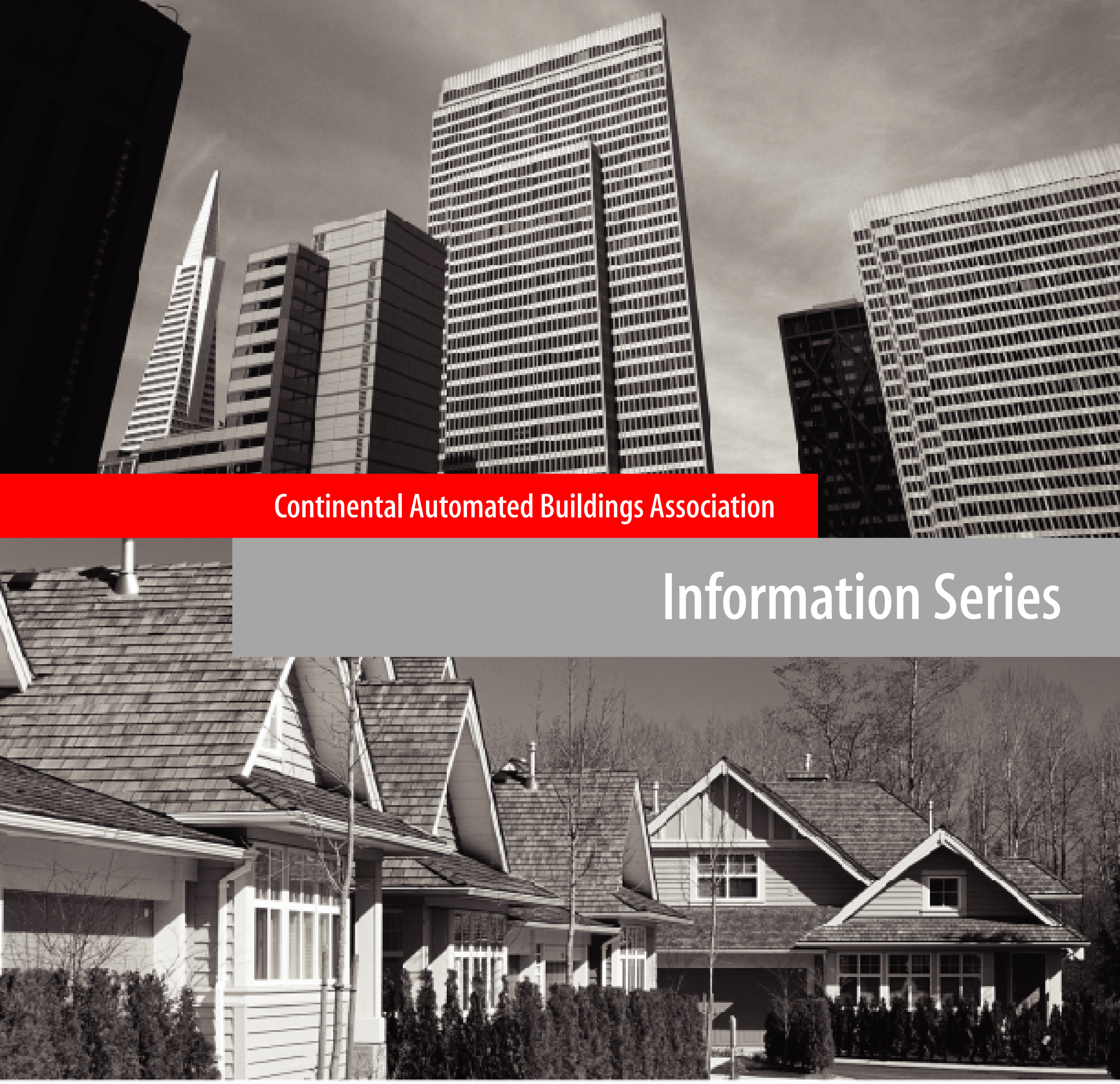


Continental Automated Buildings Association

Information Series

IS 2003-30

Many Happy Returns - The ROI of Security

CABA
www.caba.org

Many Happy Returns - The ROI of Security

Report Date: August 2003

Reprint Date: December 2003

This report was developed by Certicom, and is published by CABA with permission from Certicom. CABA expresses its appreciation to Certicom for making this report available to be included as part of CABA's INFORMATION SERIES.

Neither Certicom, nor CABA, nor any other person acting on their behalf assumes any liability with respect to: the use of, or for damages resulting from the use of, any information, equipment, product, method or process disclosed in this report.

certicom™

Many Happy Returns

the ROI of security

The Certicom 'Got Security?' White Paper Series

August 2003

Investing in Security

For manufacturers of communication devices and developers of applications, security has become an unavoidable imperative. More than ever, their customers – enterprises and network operators – require sophisticated security features.

Enterprises demand that the mission-critical communications transmitted over their internal and external networks, wireless or wired, be protected from malicious attacks and security breaches. Nowhere is this truer than in the government, health care and financial sectors, where security standards are mandated given the absolute necessity of confidentiality. At the same time, operators–telecom, wireless, cable, satellite radio and others – demand authorization and access-management features that allow them to offer differentiated services to their clientele.

Manufacturers and developers face the challenge of satisfying these customer needs while ensuring that any technology investment they make will deliver the returns they require for their own business growth and prosperity. Whether they choose to embed these security solutions into their devices or integrate them as add-on components,[1] there is no question that security functionality is a leading priority.

This white paper explores the decision-making process manufacturers and developers must undertake before committing to an investment in security enhancements. It defines the basics of a return-on-investment (ROI) calculation; presents a framework companies can use to evaluate the likely return on a security investment; defines typical business scenarios that drive the decisions to undertake security initiatives; and maps ROI fundamentals and business scenarios together to illustrate where short-term and longer-term ROI begin to emerge. Finally, the paper presents practical cases that demonstrate how the ROI framework might be applied by manufacturers and developers with particular business challenges.

ROI Fundamentals

Before undertaking any major security initiative, manufacturers typically conduct an ROI analysis, anticipating the nature and degree of return the company can expect from its investment. Will security functionality allow the organization to enter new markets, increase competitiveness, protect a revenue stream, save on the cost of conducting field upgrades or meet emerging standards and technology imperatives?

At its foundation, an ROI assessment involves calculation of the cost of the proposed initiative and of the savings and/or revenue its implementation will deliver. Other critical factors must be

[1] For more detail on embedded security for constrained devices, please refer to The Inside Story Embedded Security for Constrained Devices, the first white paper in The Certicom "Got Security?" White Paper Series.Visit **www.certicom.com/gotsecurity** for your copy.

considered as well, such as compliance with an industry-mandated technical standard such as the Federal Information Processing Standard (FIPS 140-2), a US government security requirement, and risk mitigation.

The following framework presents all ROI considerations, in four key categories: **The Investment, Quantitative Returns, Qualitative Returns and Other Considerations.** Those listed under The Investment address the expense associated with the security initiative. Quantitative Returns encompasses the financial benefits, and Qualitative Returns the non-financial ones. Other Considerations captures additional critical factors such as risk.

Given the broad range of potential technology solutions manufacturers and developers may adopt and the variation in business scenarios, it is difficult to provide a detailed calculation of the returns in real dollars. Nonetheless, by working through the ROI framework and mapping the output to the ROI grid that follows, companies can gain a strong sense of the returns to be gained through investment in security technology.

ROI Framework

To evaluate the nature and degree of ROI they can expect from an investment in security technology, organizations should answer the following questionnaire:

THE INVESTMENT

the expense associated with acquiring security capabilities

Expense

What is the required capital outlay to purchase an off-the-shelf security-enhancement product or toolkit?

Development Time

What amount of time will we need to devote to planning, development, documentation, code support and testing? For example, the expense of open source security may be zero, but it could take months of a developer’s time to integrate it or optimize it for a device.

Term for Investment

Will this initiative require a short-term expenditure or ongoing investment over the longer term?

QUANTITATIVE RETURNS

the financial benefits

Revenue

Will the new technology allow us to create new services for our customers and, therefore, to generate new revenue? Will it enable us to enter new markets, penetrate new verticals or protect a well-established revenue stream?

Cost Savings

Will we reduce our technical support costs? Our development and administration costs? Our personnel requirements? Will we access other savings?

Operational Efficiencies

Will the new technology enable us to automate business processes? To serve our customers more efficiently? Will it simplify our administration process? Optimize the productivity of individual employees and the company in general? For example, secure Internet connections have automated much of the supply chain for many industries.

Timeframe for Payback

Will we begin to realize cost savings or gather new revenue in the short or long term?

QUALITATIVE RETURNS

the non-financial benefit

Customer Value Perception

How will implementation of this new technology improve the customer experience or customer satisfaction? Will this initiative improve current and prospective customers' perception of the value of our products and/or services?

Standards Compliance

Will this technology enable us to comply with a mandated industry standard?

Product Differentiation

Will this initiative enable us to improve our competitive position and differentiate our products in the marketplace?

Focus on Core Competencies

Will acquiring security enhancements from a supplier allow us to expand our client offering while remaining focused on our core business and strengths?

OTHER CONSIDERATIONS

additional critical factors

Risk

What degree of risk are we exposing our company to with this investment? Without this investment? What are the risks we must consider before proceeding—legal, financial or other? How can we mitigate these risks?

Public Opinion

Will this initiative enhance the company's public image?

Business Scenarios

The exercise of estimating return on investment will differ for each company based on the nature of its business, the stage of evolution of its product or service portfolio, and its objectives related to the implementation of security functionality. Following are four typical scenarios.

Scenario 1

Business Objective: *Renewal*

A manufacturer or developer seeks to reduce cost and raise quality of a product or service. This scenario typically requires shorter-term investments using more mature, widely accepted technologies. Example: a successful product needs to be updated to meet today's standards or requirements.

Scenario 2

Business Objective: *Process Improvement*

A company wants to improve operational efficiency. This scenario usually necessitates shorter-term investments using new technologies. Example: adding a new anti-cloning capability to protect a revenue stream.

Scenario 3

Business Objective: *Transformation*

A company wants to replace inadequate core infrastructure. This typically requires longer-term investments using more mature, widely accepted technologies. Example: finding a new, more efficient way to complete a business process.

Scenario 4

Business Objective: *New-business Creation*

A device manufacturer or applications developer wants to invest in new business opportunities. This usually necessitates longer-term investments using new technologies.

Example: entering a new market with a new product or an existing product that has been substantially modified to meet a new customer need.

BUSINESS OBJECTIVE	ROI TIMEFRAME	TECHNOLOGY TYPE
Renewal	short term	mature, widely accepted
Process Improvement	short term	new technologies
Transformation	long term	mature, widely accepted
New-business Creation	long term	new technologies

Figure 1: *scenario summary*

Mapping ROI

In conducting an ROI assessment, a company may find the following grid helpful – to visualize where the payoffs from security investments will materialize. The x axis captures the ROI timeframe, from short to long term. The y axis captures the technology solution. This might include well-established general protocols such as IPSec or Secure Socket Layer (SSL), or specific new cryptography techniques such as Elliptic Curve Cryptography (ECC). The contents of each quadrant represent the returns to be realized at those points of intersection.

1. **Define the scenario.**
   As a first step, the company should highlight the quadrant that best reflects its primary business objective–renewal, process improvement, transformation or new-business creation.

2. **Note the returns.**
   Next, observe the returns to be accrued in that particular quadrant. In each case, a primary quantitative return can be expected, with additional qualitative returns. In every quadrant, the other considerations such as risk need to be considered.

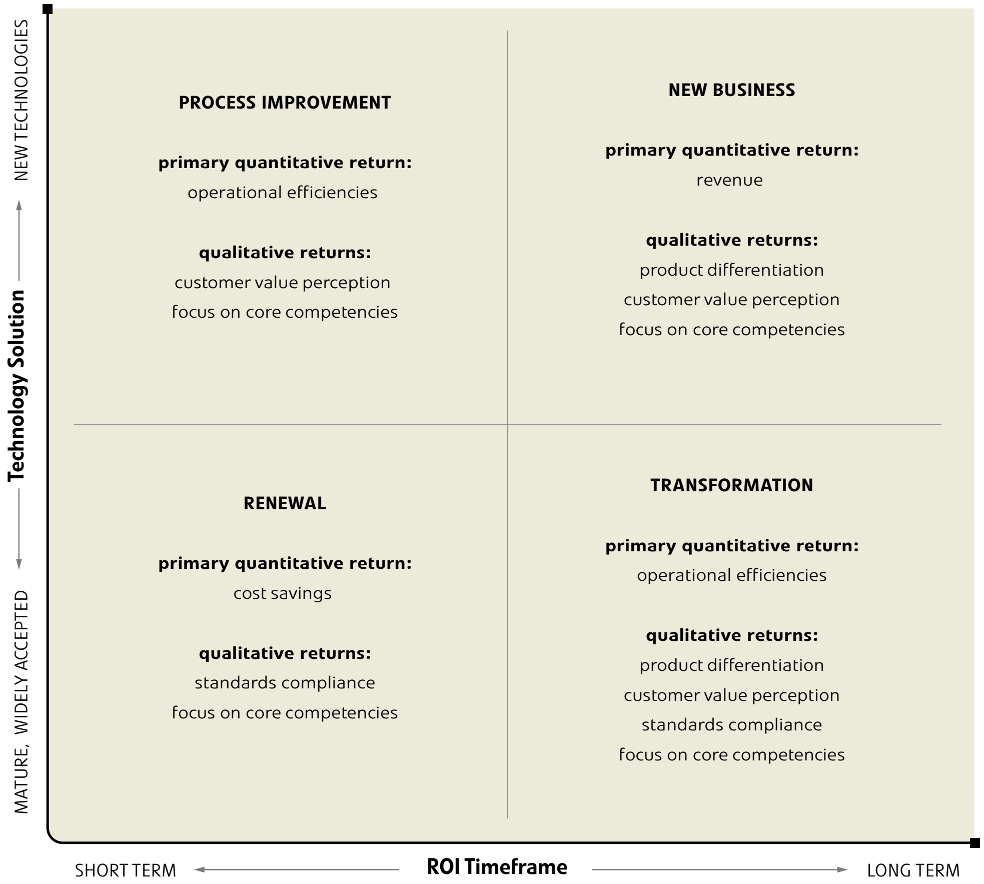
3. **Consider the axes.**
   Now, discover the timeframe for payback, and the type of technology you'll need to adopt – from established to new technologies.

4. **Assess the results.**
   Organizations *renewing* their business approach can adopt widely accepted security technology to realize short-term cost savings, primarily through operational efficiencies, while achieving standards compliance.

Companies seeking to *improve their processes* can adopt new technology over the short term to access operational efficiencies. They can also expect to realize some cost savings and to generate a certain amount of revenue from their security initiative, while meeting technology imperatives.

Device manufacturers or application developers wanting to *transform their infrastructure* can adopt established security technology to access operational efficiencies through increased productivity over the longer term, differentiate their product or service offering, and improve customers' value perception.

Finally, companies *creating new products or services* can adopt new technology to realize revenue growth primarily, as well as product differentiation, improved customer value perception and increased productivity, all over the long term.



PROCESS IMPROVEMENT

primary quantitative return:
operational efficiencies

qualitative returns:
customer value perception
focus on core competencies

NEW BUSINESS

primary quantitative return:
revenue

qualitative returns:
product differentiation
customer value perception
focus on core competencies

RENEWAL

primary quantitative return:
cost savings

qualitative returns:
standards compliance
focus on core competencies

TRANSFORMATION

primary quantitative return:
operational efficiencies

qualitative returns:
product differentiation
customer value perception
standards compliance
focus on core competencies

***Figure 2:** mapping ROI*

ROI Calculator

Since the variation in business scenarios may be infinite, no detailed calculator can be provided to calculate returns in real dollars. Nonetheless, the following format can be used to guide you in the development of your own ROI model for security investments.

1. Compile all relevant financial metrics for the Investment.

Expenses

- Estimated cost oftools and/or applications required to build in security:
- Estimated developer person months (DPMs) x monthly rate for developer:
- Estimated licensing fees charged per product, platform and/or developer:
- Estimated cost of source code (may be required to do the integration and would be an additional software cost):
- Estimated customer support costs (need to consider service level agreement with commitments around bug fixes according to severity levels):
- Estimated maintenance fees (updates and upgrades):
- Estimated royalties payable—per device, product or application, or paid upfront as a flat fee:
- Estimated consulting services for customization:
- Estimated training costs (from provider or third party):
- Marketing, sales and support costs (especially if you are entering a new market):
- Ongoing costs (keeping security current with evolving standards or market demands):

TOTAL EXPENSES

2. Compile all relevant financial metrics for the Quantitative Returns.

Revenue Increase

- Estimated increase in sales within existing markets — percentage of current revenue:
- Estimated increase in sales by entering a new market — expected market share (percentage) x the size of the new market:
- Estimated revenue that will be retained through the security investment — percentage retained of revenue in jeopardy:

OR

TOTAL REVENUES

Cost Savings and/or Operational Efficiencies

Estimated reduction in operational costs—namely:

- Personnel (any reduction or reallocation of required resources):
- Technical support (more cost-effective maintenance and upgrades):
- Development costs (quicker development cycle or reduction in required resources):

TOTAL COST SAVINGS

3. Determine your payback period.

Annualized return: Returns / Term
Payback period: Investment / Annualized Return

PAYBACK TERM

4. Calculate your ROI.

ROI = (Quantitative Returns - Investment) / Investment

ROI

5. Assess the qualitative returns and other considerations.

The ROI calculation should also take into account the non-financial benefits expected, as well as risk considerations.

Case studies

To truly appreciate how the ROI framework functions, it is helpful to see it applied to legitimate business scenarios. The four cases below outline the business challenges of particular companies, present security solutions that meet their needs, then assess their ROI.

Sample Scenario 1: Renewal

A government supplier seeks to sustain its revenues through continued delivery of security solutions to its government clients.

Background

Any manufacturer or developer wishing to sustain its government revenue base must ensure ongoing adherence to established industry standards. In the government sector, this includes FIPS as well as the incoming common access card (CAC) standard, which itself is FIPS-validated. The high cost of achieving FIPS 140-2 validation is a key challenge.

Security solution

Government suppliers must acquire a cost-effective FIPS-validated encryption technology – specifically, a cryptography module that performs both public key (verification and encryption) and private key (signing and decryption) operations, and provides:

- an inherently trusted digital signature from a trusted root authority;
- privacy and confidentiality through encryption, so information stays private at the application level;
- non-repudiation capability so digital signatures can be applied in adherence with established privacy policies, to ensure no tampering and indisputable proof of a message’s originator.

By acquiring a module that has already earned FIPS 140-2 validation, government suppliers will save themselves the time of going through the validation process on their own – which takes 9-12 months on average – and avoid the work, which can be 24 developer person months or more, of defining valid algorithms and platforms; developing the module; testing the implementation; and ongoing efforts as it passes through the validation process which include working with the third-party lab and responding to NIST’s comments and questions.

In addition, they can benefit from a cryptographic application that supports the CAC card by permitting physical and virtual authentication, enabling personal credentials to be ported from the desktop to a VPN to a PDA, wirelessly.

ROI assessment

By adopting a sophisticated FIPS-validated cryptographic solution, the government supplier can meet the security requirements of its customers in a cost-effective way, ensuring adherence with technology imperatives, and save two years of development and validation effort resulting in significantly faster time-to-market.

Sample Scenario 2: Process Improvement

A printer manufacturer seeks to preserve its revenue stream.

Background

Printer manufacturers—like network equipment vendors, fax machine makers and others—make a good proportion of their revenue from the sale of aftermarket replacement supplies; in this case, ink cartridges. Once a printer is sold, printer manufacturers rely on customers' ongoing purchase of refill cartridges for sustained revenue.

Threatened by competition from suppliers of aftermarket clone cartridges, printer manufacturers seek ways to discourage customers from purchasing substitutes.

Security Solution

Manufacturers must adopt digital-signature technology that will enable their printers to reject clone cartridges. Using public key technology within a security toolkit, manufacturers can incorporate software mechanisms into their printers that:

- provision a unique manufacturer's digital signature for each cartridge;
- have the printer authenticate the cartridge's unique digital signature;
- have the printer optionally challenge a 'smart' tamper-proof cartridge for validity; and
- provide for other means of intelligence in the printer to ascertain illegitimate print cartridges.

ROI Assessment

By adopting this approach, the printer manufacturer sustains its revenue stream, accesses operational efficiencies—the act of policing clone activity is radically simplified—and is able to return its focus to its core competency: printer design and manufacture.

Sample Scenario 3: Transformation

A cable modem manufacturer wants to increase its service-provider customer base.

Background

In the fiercely competitive cable modem market, OEMs seek to gain an edge by supporting service providers with added value. A key way for them to do so is to help cable operators overcome the problem of fraud: many clone modems are sold into the marketplace, enabling individuals to steal cable Internet service from providers.

Security Solution

Manufacturers can help service providers overcome this challenge by offering a modem product that not only integrates with service providers' existing infrastructure but also meets the requirements of DOCSIS v1.1 and eventually v2.0, an open standard for broadband networks established by CableLabs, the body regulating the North American cable industry. DOCSIS was created to ensure that cable equipment from different manufacturers could and would interoperate.

Cable manufacturers need to access a DOCSIS-compliant digital cryptographic solution that enables them to install digital certificates in their modems, so the modems can authenticate themselves to the service provider network—preventing modem-clone activity and fraud.

ROI assessment

By incorporating a security toolkit that offers service providers DOCSIS-compliant authentication capability, the cable modem manufacturer can gain differentiate their product offering, increase service providers' perception of the OEM's value and meet the DOCSIS technology imperative while focusing on core competencies.

Sample Scenario 4: New-business Creation

A manufacturer of wireless handhelds seeks to differentiate itself from competitors, break into the enterprise market and preserve its margins.

Background

Faced with increasing competition and eroding customer-rate structures, wireless handheld manufacturers seek to generate new revenue by offering service providers built-in security functionality for individual consumers; and security features demanded by enterprise customers. At the same time, they seek to minimize their administrative costs and ensure only its own applications are used on its devices.

Security Solution

By embedding new security functionality, such as a cryptographic service provider (CSP) on the chip, or by bundling security applications with the device, the manufacturer can offer sophisticated cryptographic functionality that will protect mission-critical enterprise communication. The ultra-compact CSP optimizes system resources and allows manufacturers to build security directly into their devices, efficiently and economically.

Using code signing, the manufacturer can program its devices to ensure only its code upgrades are accepted. This protects the devices from being compromised by malicious code from an untrusted party and facilitates over the air provisioning by providing a valid signature linked to a trusted root key.

ROI assessment

By implementing new security technology, the wireless handheld manufacturer will open a new revenue stream, differentiate their product offering, improve the customer experience and customers' perception of value and focus on core competencies.

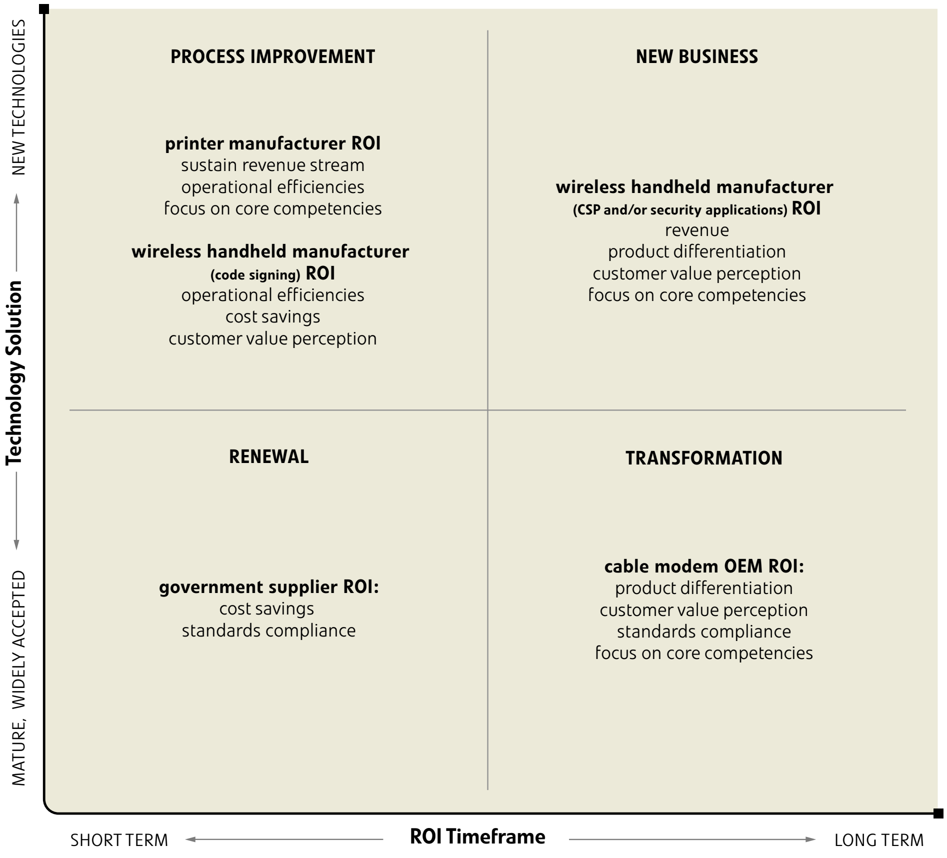


Figure 3: **the payoffs**

By adopting mature security technology, the government supplier will meet the technology imperatives of the government sector and sustain its revenue stream in the short term. By adopting leading-edge cryptographic technology, the wireless handheld manufacturer will access new revenue streams and increase its value to service providers over the longer term.

By acquiring wireless-update capability, the company will gain operational efficiencies, realize valuable cost savings and improve service providers' perception of value.

Conclusion

Any responsible company considering a significant capital investment first undertakes a comprehensive analysis of the likely return on investment. Device manufacturers and application developers are no different. Those seeking to gain a competitive advantage and access new revenue by embedding security in their communication devices and electronics components, must evaluate several key criteria before they can determine if a technology investment will help them sustain and grow their businesses.

The detailed ROI framework presented in this paper lays out those criteria and offers companies a tool to clarify the benefits they can expect to realize from a technology investment, assess the risks involved, and recognize when payoffs will begin to materialize.

As the sample cases presented demonstrate, with proper planning companies can realize significant benefits—revenue growth, productivity gains, improved customer value perception and more. They can overcome their business challenges and successfully improve their competitive position.

Other Certicom "Got Security?" White Papers

The Inside Story: Embedded Security for Constrained Devices

Welcome to the Real World: Embedded Security in Action

These white papers are all available from **www.certicom.com/gotsecurity**

About Certicom

Certicom is a leading provider of wireless security solutions, enabling developers, governments and enterprises to add strong security to their devices, networks and applications. Designed for constrained devices, Certicom's patented technologies are unsurpassed in delivering the strongest cryptography with the smallest impact on performance and usability.

Contact Certicom

Corporate Headquarters

5520 Explorer Drive
Mississauga, Ontario
L4W 5L1
Tel: +1-905-507-4220
Fax: +1-905-507-4230
E-mail: info@certicom.com

Sales Offices

Canada

5520 Explorer Drive
Mississauga, Ontario
L4W 5L1
Tel: 905-507-4220
Fax: 905-507-4230
E-mail: info@certicom.com

Ottawa

84 Hines Road
Kanata, Ontario
K2K 3G3
Tel: 613-254-9270
Fax: 613-254-9275

US Western Regional Office

1810 Gateway Drive, Suite 220
San Mateo, CA 94404
Tel: 650-655-3950
Fax: 650-655-3951
E-mail: sales@certicom.com

US Eastern Regional Office

1175 Herndon Parkway, Suite 750
Herndon, Virginia 20170
Tel: 571-203-0700
Fax: 571-203-9653
E-mail: sales@certicom.com

Europe

Golden Cross House
8 Duncannon Street
London WC2N 4JF UK
Tel: +44 20 7484 5025
Fax: +44 20 7484 5150

www.certicom.com