



# ANNUAL PLANNING TO OPTIMIZE ENTERPRISE INFORMATION SECURITY



ISO 9001:2008 Certified

60 Commerce Street, Suite 1100 • Montgomery, AL 36104 • USA  
T: 877.ICS.INC9 / 334.270.2892 • F: 334.270.2896 • info@ICSInc.com

[www.ICSInc.com](http://www.ICSInc.com)



© 2012 Integrated Computer Solutions, Inc. All rights reserved. Rev. 0112



A vital part of planning a successful year is to take active measures to protect your organization's information and technology infrastructure. ICS can help.

---

877.ICS.INC9 | [www.ICSInc.com](http://www.ICSInc.com)

# ANNUAL PLANNING TO OPTIMIZE ENTERPRISE INFORMATION SECURITY

At one time, information security was as simple as a unique ID and the watchful guard of the onsite ops team. But the threats your organization faces today are unseen and uncontained, and increased demands of regulators present challenges unmatched at any previous point in time. A strategy as simple as those employed in the early days will result in fireworks—just not the kind you typically enjoy when ringing in the new year.

A vital part of planning a successful year is to take active measures to protect your organization’s information and technology infrastructure. With threats ever-evolving and the financial and collateral costs of a breach continually on the rise, a comprehensive security strategy is an essential resolution.

## TABLE OF CONTENTS:

<b>Straight Talk: Why Is Annual Planning So Important .....</b>	<b>4</b>
Reason #1: Threats Evolve .....	4
Reason #2: The Cost of a Breach is on the Rise .....	5
Reason #3: It Pays to Be Proactive .....	6
<b>The Integrated It Security Plan: How ICS Can Help .....</b>	<b>7</b>
<b>THE 2012 IT Security Annual Planner .....</b>	<b>9</b>

*Learn out more about the business-minded, security-focused solutions ICS offers, including Incident Response, Business Continuity Planning and Disaster Recovery. For more information, visit [www.ICSI.com](http://www.ICSI.com).*

## STRAIGHT TALK:

# WHY IS ANNUAL PLANNING SO IMPORTANT?

## REASON #1: THREATS EVOLVE

**Threats evolve. Every year they become more advanced, more numerous, and approach from more points of entry.**

New advances in software, web applications, cloud computing and virtualization technologies have created opportunities to grow and profit even in the shakiest of economies... *IF* the technologies you have invested in are integrated with the latest advances in information security.

Consider the devices that you provide your staff to enable them to work more efficiently—smartphones (with 3rd party apps), laptops, and other wireless devices, removable media and storage drives—each bring additional points of entry, thus weakening your network security *exponentially*.



## INFORMATION SECURITY RISK ASSESSMENT:

An Information Security Risk Assessment provides a detailed evaluation of your organization's IT security posture, covering everything from configuration management to media protection to audit and accountability. Consider it like checking the doors and the windows on your network. Learn more; scan the QR code to the left.

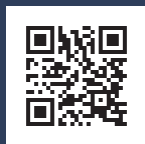
According to the SANS™ Technology Institute, “exploiting weaknesses in hardware systems is becoming a more and more attractive target area for attackers.” Additionally, the SANS Technology Institute expects that in 2012, “attackers will increasingly make use of social-engineering tactics to bypass technological security controls.” [www.sans.edu]

## REASON #2: THE COST OF A BREACH IS ON THE RISE

**The average cost of a data breach is on the rise. It never goes down.**

And let us not forget that the cost is not merely the immediate financial impact—it affects consumer confidence as well as brand equity and viability over the long term.

In 2011, the Ponemon Institute reported that the cost of a data breach had reached \$214 per compromised record and averaged \$7.2 million per data breach event. [www.ponemon.org]



### VULNERABILITY ASSESSMENT:

A Vulnerability Assessment provides a view of information that can be obtained from a scan of an organization’s network—either internally, externally, or both. This non-intrusive assessment identifies problems caused by things like poorly configured systems and unpatched software.

Research also indicates that while malicious attacks can be the most expensive, a larger percentage of breaches are caused by non-malicious activity.

### REASON #3: IT PAYS TO BE PROACTIVE

#### **Proactive measures cost significantly less than reactive ones.**

If the average data breach event costs in the ballpark of \$7 million, it would stand to reason that a thorough and strategic information security strategy would be a key part of every organization's annual budget; however, it is all too often neglected until it is too late. For a mere fraction of the cost of cleaning up a breach, a smart organization is able to conduct a complete information security health check and implement the necessary controls to keep their organization secure.



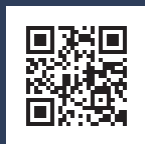
#### **WEB APPLICATION ASSESSMENT:**

Today more than ever, businesses use web-based applications for sales, marketing, accounting and other business functions. The Web Application Assessment will identify any potential security issues caused by web-based applications as installed, configured, maintained, and used in the production environment.

## THE INTEGRATED IT SECURITY PLAN: HOW ICS CAN HELP

**Consider ICS as your partner in the battle to protect your information assets.**

Start the year off with a comprehensive plan to ensure your organization is secure and operating at peak productivity. ICS consultants can help identify technical security and network performance issues within your organization, and pair those needs with exactly the right products and services to handle even the most complex enterprise information security issue. We provide industry-leading expertise to reduce risk and secure your network for the months ahead.



### PENETRATION TESTING:

Certified ethical hackers take the Vulnerability Assessment and Web Application Assessments a step further with the Penetration Test, verifying their findings and determining the impact a breach could have on external and internal networks.



**BEST PRACTICES:**  
**THE 2012 IT SECURITY ANNUAL PLANNER**



## BEST PRACTICES:

# THE 2012 IT SECURITY ANNUAL PLANNER

The chart below indicates the frequency with which standard information security assessments and activities should take place.


ACTIVITY	ANNUALLY	QUARTERLY	MONTHLY	INCIDENT DRIVEN	BUSINESS DRIVEN	PRIOR TO FIELDING
Risk Assessment	X					
COOP/DR Testing	X					
Vulnerability Assessment		X	X			
Penetration Testing		X	X			X
Web App Testing		X	X			X
Incident Response/Forensics						
Technology Insertion				X	X	
Security Education	X			X	X	
Application Code Review				X		X

**BEST PRACTICES:**

# THE 2012 IT SECURITY ANNUAL PLANNER

**Fill in the boxes below with target dates for your organization for each of the activities, referring to the best practices on the previous page.**

ACTIVITY	ANNUALLY	QUARTERLY	MONTHLY	INCIDENT DRIVEN	BUSINESS DRIVEN	PRIOR TO FIELDING
Risk Assessment						
COOP/DR Testing						
Vulnerability Assessment						
Penetration Testing						
Web App Testing						
Incident Response/Forensics						
Technology Insertion						
Security Education						
Application Code Review						



Integrated Computer Solutions, Inc. is a Security-Focused, Business-Minded IT Solutions Provider, delivering consistently high levels of client satisfaction and measurable results. ICS is unique in its market because we have an established track record of providing enterprise technology and security services to clients in the commercial field, public sector and education markets, as well as a foundation in service with the United States Department of Defense.

Learn more at [www.ICSIInc.com](http://www.ICSIInc.com).



Integrated Computer Solutions, Inc.  
877.ICS.INC9 | [www.ICSInc.com](http://www.ICSInc.com)



ISO 9001:2008 Certified