

## Banking Security Services

### How secure are your customers?

Begin by answering the following **3** questions about your financial institution:

- (1) Does your bank have a CAMELS rating of a 1?
- (2) Is your bank compliant with the Gramm-Leach-Bliley Act of 1999?
- (3) Does your bank have a Customer Information Security Program (CISP) in place?

If you answered "Yes" to all 3, your bank is more prepared than 80% of all financial institutions in the U.S. However, if you answered "No" to any of these questions, your customers and their personal information could be at risk. With new federal regulations serving as the guidelines, [we're here to help](#).

### How can we help?

- ❑ **Security Risk Assessment** - Banks deal with risk every day. With every new loan review, they profile each candidate to find out **how much risk** can be accepted and how much it costs to take on this risk. Evaluating the information technology within a bank is exactly the same. Profiling everything from data confidentiality practices to IT management capabilities to information security policies is the first step towards addressing the risk. Often the exposures can be easily corrected - but not until the problem is found can it be fixed. Asking questions and **offering solutions** is how we get started.
- ❑ **CISP Development** - So you're aware of all the risks to address - now what? The centerpiece of any world-class banking organization is a Customer Information Security Program (CISP). This is what **regulators demand** and what **investors relish**. We've worked with regulators to find out what they want and we work with clients to give them the answers. We focus on getting the CAMELS rating higher and delivering a plan that doesn't just sit on a shelf but is actively used to lower vulnerability.
- ❑ **Technology Implementations** - Keeping up with the Joneses isn't what it used to be. With the tremendous competition in the banking industry, sometimes a key differentiator is the technology used to protect and serve their customers. Having implemented systems for clients in more than 15 countries, we can help replace or augment existing technology solutions and train your staff to give your financial institution the **competitive advantage** necessary to outperform the Joneses.

### Why do it?

- ❑ **It's the Law!** - The Gramm-Leach-Bliley Act of 1999, in only 12 sentences implemented privacy statutes and protected non-public personal information. Banks are slow to comply and face uphill battle with investors and possible penalties if no action is taken.
- ❑ **Prevention, Detection, Response** - With these three words, banks can build processes to protect their customers, assets, and future profits.

**"More than half...[of] banks had done no risk assessment or an inadequate risk assessment..."**

**"The greatest threat to information security does not come from the hacker...it comes from the member of your staff who's inside the bank and doesn't have to hack in to get access."**

Source: Richard Cowden, "Privacy Stealth: Information Security Rules Escape Notice of Many Bank Officials"

### Who needs to be more secure?

- ❑ **Federal Banks** - These larger institutions typically have more employees and therefore more points of risk. Processes such as disaster recovery, temporary staff training, and password protection policies have a greater impact at these banks with lots of "moving parts." Our aim is to standardize the methods to empower the management to know how secure their bank really is.
- ❑ **State Banks** - With more limited resources, it's difficult for these institutions to build things like security programs and perform risk assessments. Trying to do their normal jobs often pushes these regulation requirements to the back burner. Therefore, we guide them through the process step-by-step in order to make it as simple as possible to become fully compliant.
- ❑ **Other Financial Institutions** - Smaller banks and credit unions know they need to set the alarms, close the vaults, and hire a police officer. Securing electronic information and assessing technology risks is more foreign to these organizations but equally important to the larger institutions.

## What actions do we take?



## Why JD Warren Associates?

- ❑ **Principled** - We use the three cornerstones of **Independence**, **Innovation**, and **Integrity** as the basis for every client engagement. We are prepared to decline engagements where these principles cannot be upheld.
- ❑ **Experienced** - We mix strategy and experience from a variety of industries and business models so we see **beyond the limits** of any single company, industry, or problem.
- ❑ **Dedicated** - We operate efficiently. Our fees are competitive. We will tell you what we think and why - always **framed by your desired outcomes** and plans. And, we stand behind the work we do.
- ❑ **Independent** - We are independent of all product vendors and binding financial arrangements. Our success is **not tied to any vendor revenue stream**, agency arrangements, or other hidden reasons why we would skew our results for anything other than what is best for you.

If you'd like to learn more about our services, contact us at **415 982 9900** or please visit our website at [www.jdwa.biz](http://www.jdwa.biz).  
Your future. Your path. Let us guide you.



**SYSTEM RENOVATION | STRATEGY & IT CONSULTING | PROGRAM MANAGEMENT | COACHING | M&A | QUALITY ASSURANCE**

**Eyes to your future... Guides to your goals... Through technology.**

# Banking Security Services

## Who?

1. Federal Savings Banks
2. FDIC-Insured Banks
3. State Chartered Banks

## What?

1. Security Assessment
2. CISP Development
3. Business Continuity Planning

## When?

1. Now!! GLB 501(b) was law as of 7/1/01
2. Prior to an M&A with another bank
3. In transition from state to federal charter

## Why?

1. It's the law!
2. To improve a bank's CAMELS rating
3. Reduce the chance of security breach

## How?

1. Using our proven methodology
2. Analyze, Select, Prioritize, Build, Launch
3. Independence, Innovation, Integrity