

How Good is Your Security?



Walls were great security solutions until ladders were invented.

The origins of the Great Wall can be traced back to 771 BC although the Great Wall as we know it comes from the Ming Dynasty (1368 AD to 1644 AD). While certainly a hindrance to slow attackers, it still required constant vigilance and garrisons of troops to repel attacks.

Risk no longer is constrained to neighboring countries. Today, attacks are less visible and originate from anywhere in the world. Computers have enriched the world with revolutionary changes in almost every facet of our lives and have enabled a quantum leap in the arsenal of tools for those who would attack us.

The Great Wall relied on real time monitoring and response to attacks in a time when technology provided few new weapons.

Today, new weapons are developed quickly and attacks occur in milliseconds.

Many companies delegate the role of managing information security to data processing or network support. As a result, one of the most important duties in

the company is performed by someone without sufficient knowledge or sufficient time to devote to the task. Are these common statements in your organization?

1. Automatic updates provide all needed security patches.
2. Intelligent, trusted employees understand good security practices.
3. An alarm system eliminates theft.
4. Hacking is not a concern as we have nothing of value.
5. Our firewall protects us from malicious Internet activity.
6. Sensitive data is never lost.
7. We never had a security incident that needed action.
8. The information we have is of no value to identity thieves.

None of the above is true.....

Do you need a major accounting firm to send in consultants? Probably not but you do need someone to provide expert advice and support when you need it.

SERVICES

We believe that security needs to be an integral part of every organization and it must be affordable. Our services allow you to have customized security services and a dedicated Security Officer with a fixed cost agreement. Services under this agreement include:

- Gather information to create a security risk profile for your systems.
- Provide customized security patching guidance detailing when and where patches are necessary. Alternative controls may be recommended if they offer less costly but effective solutions.
- Supply a monthly security awareness newsletter to educate employees about their responsibility to protect company assets and prevent losses.
- Provide consultation to identify best practice security solution as needed.
- Help create comprehensive security programs to share with employees and support organizations.
- Assist with proactive audit preparation and design effective remediation's which balance business processes and security concern.
- Provide recommendations and guidance for regulatory compliance.

These services will be provided under a fixed cost monthly service plan.

Customized service packages will be provided upon request. Please call (1-516-306-2539) or email (davidk@cdfsecurity.com) for more information.

We also offer specialized security services to support compliance requirements and supply metrics for your security infrastructure:

- HIPAA compliance analysis.
- Evaluate alignment with the PCI standard.
- Develop and document a comprehensive security architecture including effective hardware and software counter-measures.
- Perform penetration tests (internal and/or external attacks).
- Review existing security programs and policies.
- Source code review.
- SOX compliance program.
- Targeted vulnerability assessments.
- Web server security assessments including the identification of SQL injection risks.
- Forensic analysis and evidence collection for security issues.

ETHICS

We strive to provide optimum, cost effective solutions to mitigate risk.

We have no affiliation with any product or service we may recommend and do not accept commissions, fees or any other valuable considerations from vendors.

All raw data, analyses, and recommendations are held in strict confidence to the extent permitted by law.

BACKGROUND

Founder David Kapusta was employed by Alcoa for fifteen years and served as Alcoa's global Security Architect for over ten years. In this capacity, he designed and managed Alcoa's global security infrastructure and authored a comprehensive Security Policy for Alcoa.

Alan Levine, the Chief Security Officer at Alcoa, Inc. wrote:

"During his years in Information Security, Dave has been integral to every improvement we've made in security policy, protocol, technology, and organization. He has been key to addressing every challenge, to putting out every fire and to paving the road for long term success."

Prior to joining Alcoa, Dave worked on process control systems and optimization of manufacturing processes.

CONTACT

We are located in New York and service organizations both large and small.

**CDF Security, Inc.
PO BOX 1229
Long Beach, NY 11561**

email: davidk@cdfsecurity.com