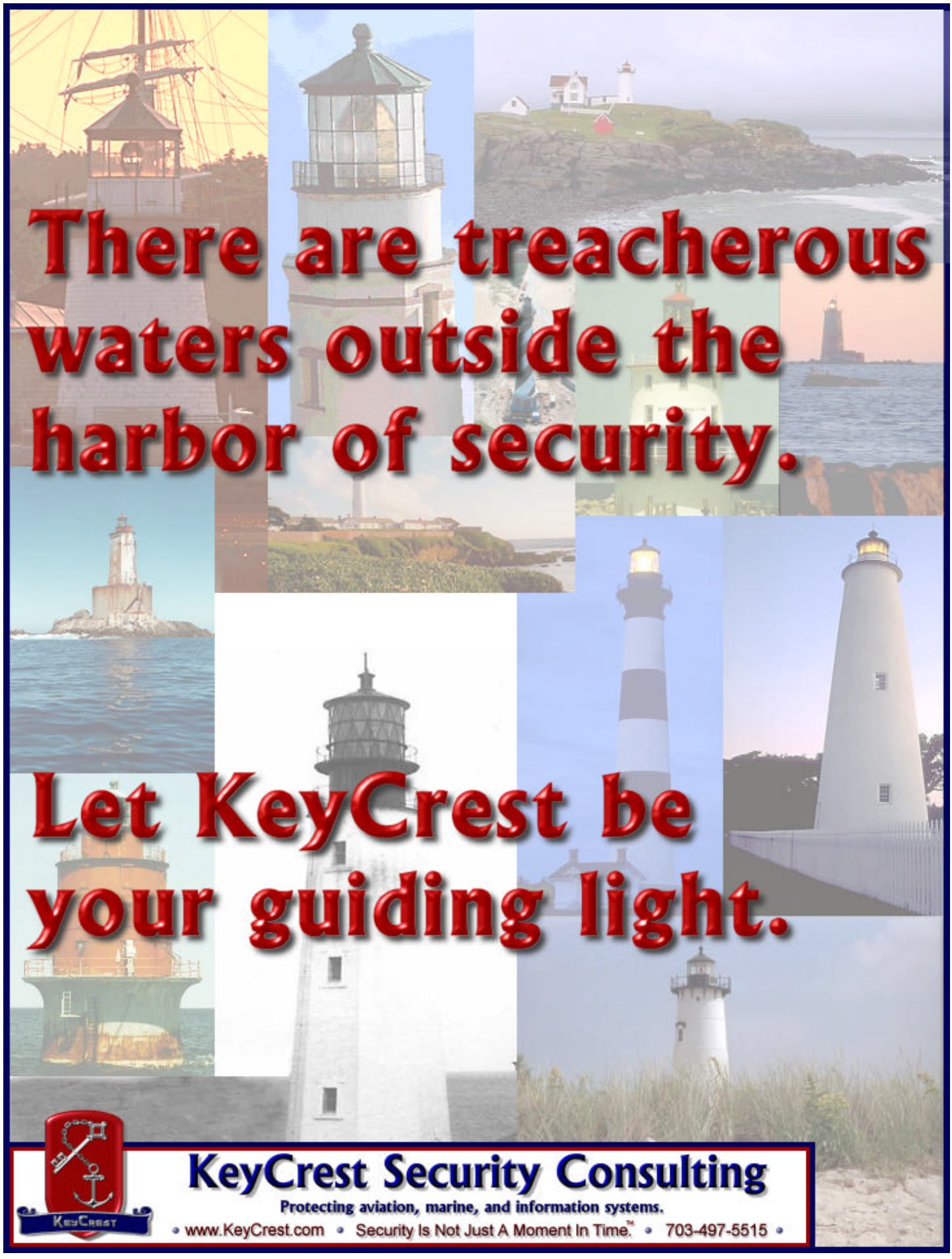
There are treacherous waters outside the harbor of security.
Let KeyCrest be your guiding light.
KeyCrest Security Consulting
Protecting aviation, marine, and information systems.
• www.KeyCrest.com • Security Is Not Just A Moment In Time.™ • 703-497-5515 •

KeyCrest Services

Security Program Management

- Project administration
- Security configuration management
- Management briefings
- Cost-benefit analyses

Best Practices

- Risk and vulnerability assessments
- System certification and accreditation
- Policies and procedures
- Operational evaluations and audits
- Security architecture and benchmarks
- Web design and secure reengineering

Technical Services

- OS and system hardening
- Scanning and penetration testing
- Implementation of anti-virus strategies
- Countermeasure implementation
- Wireless security

Incident Analysis and Response

- Incident prevention and forensics
- Business continuity and disaster recovery planning
- Identification and removal of malware
- Evidence recovery and retention

Standards and Regulatory Consulting

- HIPAA Audits
- PDD-63 and regulatory compliance
- Privacy Act
- Accessibility (Section 508) compliance

Products

- Chemical, biological, and nuclear detection
- Personal firewalls and IDS
- Enterprise E-mail, Firewall, IDS appliance
- Behavior and policy-based IDS
- Automated Risk Assessment Support Tools

Management Team

Thomas M. Brown, CISSP, is KeyCrest's President and CEO. He is a former Program Manager for the Federal Aviation Administration (FAA) with over 30 years of experience in information systems. Until late 2001, he was the Information Systems Security Manager and Webmaster for the Regulation and Certification business at the FAA. Mr. Brown's career includes leading multi-million dollar information security programs, managing a national technical support operation, data center operations management, computer system design, analysis, and programming. His academic work includes four years study toward a BS in Mathematics.

Laurie McQuillan, CISSP, is Vice President of KeyCrest. She is an experienced consultant and manager with a 25 years' experience in Government and commercial information technology, information security, data management, acquisition support, accounting, budgeting, and project and program management. Ms. McQuillan has a Master of Science in Information Technology Management and a CIO Certificate from the Federal CIO Council's GSA-sponsored CIO University program. She is the author of articles on information security and a guest lecturer at Capital area universities.

Field Locations

Austin, TX

Ft. Lauderdale, FL

Oklahoma City, OK

Atlanta, GA

KeyCrest

KeyCrest Security Consulting

Corporate Headquarters:
P.O. Box T-0375
Woodbridge, VA 22194

Phone 703-497-5515
Fax 703-499-9316
www.KeyCrest.com

Program Management

Project and program administration: Many security programs have grown rapidly in the past few years, and have evolved to address the changing landscape of security threats. KeyCrest consultants collectively have over a hundred years managing these programs and ensuring that growth and change are appropriately focused. KeyCrest can assess which aspects of your program deserve the most attention, and when you are faced with budget and staff constraints can help you decide where to focus those scarce resources.

Security configuration management: IT professionals are well-versed in configuration management and in the need to manage technical and organizational change. KeyCrest consultants have developed security-specific configuration management processes which can be seamlessly melded with your IT management program.

Fraud management and control: The fraudulent use of technology and information is a rapidly-growing problem, one which the legal and law enforcement communities are struggling to respond to. KeyCrest can help you prevent fraud before it happens by looking for vulnerabilities in your infrastructure and recommending correction.

Intellectual property protection: When you invest your time and money in developing a product or service, you want to protect it from theft, copying, misuse, and other problems. KeyCrest can help protect your intellectual property by recommending safe methods for managing it and recommending appropriate steps for preventing misuse.

Management briefings: Approaching senior management to advise them on your security program can be daunting, even more so if you are asking for resources or presenting difficult news. KeyCrest can help craft briefing packages which capture management attention, put issues in perspective, and help persuade your audience to understand your views.

Cost-benefit analyses: There is an axiom in the security world that says you should not spend more to protect an asset than the asset is worth. KeyCrest can help you decide between competing alternatives for protection by assessing the costs and values of the systems and information you are securing.

KeyCrest Corporate Capabilities

Best Security Practices

Risk and vulnerability assessments: Determine what vulnerabilities exist in your technology infrastructure, the threats that might take advantage of those holes, and the likelihood that any threats might act. KeyCrest consultants have performed hundreds of risk assessments for commercial and government organizations.

System certification and accreditation (C&A): To certify an IT system, you must identify the security requirements for the system and determine whether those requirements are being met. If not, a remediation effort is required to correct any security shortfalls. With the documentation that results from this effort, a management official can formally take accountability for the system's security posture. Federal regulations require that mission-critical applications be certified, but C&A is a good idea for any organization, because it gives you a baseline from which to operation and maintain each system securely.

Product evaluation: All vendors believe their security products are the best on the market. How do you know which claim to believe? KeyCrest can perform an independent assessment of security products and help you determine which will best meet your requirements.

Policies and procedures: A well-crafted security policy is the keystone of any information security program. Without a good policy, your end users, system owners, and other constituents do not know what security requirements they must follow in carrying out their day-to-day work. KeyCrest can create a policy for you or can review existing policies to ensure that you are protected. We can also create guidelines and procedures to support your policy or other requirements.

Operational evaluations and audits: Technology changes quickly, and an operation that is secure today may not be secure tomorrow. KeyCrest can audit your operations to find any holes in their security and to verify that security requirements are being met.

Security architecture and benchmarks: When you are building a home, your architect draws a blueprint for the work to be done. KeyCrest can create such a blueprint for your security program or specific parts of it. With this blueprint, we can benchmark technologies and approaches to implementing a strong and secure environment.

Web design and secure reengineering: With the growth of e-commerce and e-government have come increasing threats to online operations. KeyCrest can design a strong, secure web site for you or can re-engineer your existing Internet presence to close any holes in its security.

KeyCrest Corporate Capabilities

Technical Services

Wireless strategy and architecture: One of the most exciting recent developments in the IT arena is the ability to communicate between devices without cables and wires. But every new technology brings new threats. KeyCrest can help you develop a wireless architecture and an implementation and rollout strategy to safely take advantage of wireless technology.

Wireless LAN protection: The term "sniffer" refers to hardware or software that can intercept network traffic and help determine its contents. As wireless networks proliferate, sniffers can be used successfully just by driving by a wireless LAN facility. KeyCrest can assess your wireless networks and perform 802.11b compliance audits. We can recommend and implement steps for protecting you against sniffers and for operating your LAN securely.

Operating system hardening: There are dozens of "best practices" on the market to describe how to lock down your operating systems. KeyCrest consultants have assessed many of these practices and synthesized them into the "best of the best". We can adapt these practices to your environment and create an organization-specific lockdown process that is sustainable over time.

Scanning and penetration testing: Many hackers use scanning and penetration tools to look for vulnerabilities in your infrastructure. KeyCrest can help you "see" what the hackers see by using sophisticated and advanced technologies. Further, we can use the results of this testing to create a specific security remediation plan for you.

Implementation of anti-virus strategies: The anti-virus segment of the IT security industry is one of the fastest growing today, as viruses proliferate and threaten new platforms and technologies. KeyCrest will help you sort through your anti-virus options and recommend an appropriate strategy for protecting every part of your infrastructure from destructive intrusions.

Personal firewalls: It may no longer be sufficient to place a firewall in its traditional place between your network and the world wide web. Now, many threats come from internal sources and already have access to your network, and other threats cannot be stopped by traditional firewalls. KeyCrest can help you implement a firewall on your personal workstation, protecting you from threats regardless of their source.

Countermeasure implementation: New vulnerabilities are discovered all the time, requiring that you respond rapidly with countermeasures to protect against exploits. KeyCrest can perform security remediation on the fly when serious vulnerabilities are found. We can also create and implement specific countermeasure plans for systems, networks, and other technology.

Incident Analysis & Response

Incident prevention and forensics: In an ideal world, we all want to prevent security incidents before they happen. KeyCrest can recommend and put in place a process for preventing security incidents, for detecting incidents and stopping them before damage occurs. But if the worst *does* happen, KeyCrest can help diagnose what happened and why, and can manage the incident recovery process.

Incident response center operations: Many organizations are creating their own "CSIRC", or Computer Security Incident Response Capabilities. KeyCrest consultants have authored documents to establish CSIRC concept of operations and management methodologies, and can help establish, manage, staff, and operate an incident response organization.

Disaster recovery planning: Most of us want to believe that disasters will only happen to "other people". But world events have proven us wrong – disasters *do* happen, and they can hit close to home. KeyCrest can help you establish a plan for responding to disastrous events, whether they are natural – like floods, man-made – like electrical failures, or political – such as terrorist attacks.

Identification and removal of malware: Viruses, Trojans, and other malicious code can strike in a matter of micro-seconds, or can hide in your infrastructure and strike months later. KeyCrest can help analyze your IT resources to determine whether they are free of this code, and if malware is found, we can remove it.

Disk analysis and recovery: When security incidents happen, you may lose critical business information. However, sometimes the information can be recovered, even from disks which appear damaged. KeyCrest can analyze your storage devices to determine recoverability, and can reclaim your information when it's possible to do so.

Evidence recovery and retention: Because cyber-crime has grown so quickly, law enforcement agencies are still developing techniques for collecting and storing evidence and using it in prosecutions. KeyCrest can help you understand the latest requirements and can suggest ways to preserve crucial evidence safely.

KeyCrest Corporate Capabilities

Standards and Regulations

HIPAA Audits: The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), also known as HIPAA, is not a "technology law", but it has significant implications for the way in which organizations manage health care information because it creates stringent protection requirements for patient data and holds violators of the Act accountable for mishaps. KeyCrest can audit your medical systems and determine whether you are in violation of the law, as well as recommend measures to achieve compliance.

PDD-63 and regulatory compliance: Presidential Decision Directive 63 prescribes ways in which the nation's critical infrastructure will be protected. All government agencies and many other organizations must follow PDD-63 and related guidance. KeyCrest consultants have significant experience with security actions needed to maintain regulatory compliance. We can help you determine what regulations apply to your environment and recommend compliance measures.

Privacy Act compliance: There are dozens of public laws that regulate how information must be protected and safeguarded. These include the most well-know Privacy Act of 1974, which is a "code of fair information practices" that regulates the collection, maintenance, use, and dissemination of personal information by federal government agencies. There are related regulations that apply to non-federal agencies and to commercial organizations. KeyCrest can help you assess whether any aspect of your infrastructure threatens compliance with any of this legislation, and can take steps to ensure that your information is managed with individual privacy in mind.

Accessibility (Section 508) compliance: Section 508 of the Rehabilitation Act of 1998 requires that Federal agencies' electronic and information technology be accessible to people with disabilities. Section 508 establishes requirements for electronic and information technology developed, maintained, procured, or used by the government. KeyCrest consultants have done numerous 508 assessments, and can help you revise your technology and systems to comply with the law.

KeyCrest Mission and Vision

Our mission as a company is to enhance the security of the nation, its government, and its citizens. We will do that by making professional security services and products available to organizations and individuals seeking to protect their information, aviation, and marine assets.

Our corporate vision is to grow the company into a preeminent provider of security products and services. We will do this through technical and professional leadership in our field, helping to shape the future of information, aviation, and marine security by creating innovative solutions for our clients and for the security business.

Guiding Corporate Principles

The satisfaction of our clients is our paramount goal. We will maintain this satisfaction by ensuring that client requirements are fully defined and understood, by providing the best services possible, and by seeking to meet all expectations with products and services of the highest caliber.

The nature of our business requires us to earn and maintain the trust of our clients and our employees, and the respect of our competitors. KeyCrest managers, employees, and business partners are required to adhere to strong ethical standards and to carry out their work in a manner that enhances this trust and respect at all times.

We believe that we can best serve our clients by hiring and retaining professionals who are the best in their field and by working in partnership with organizations who offer services which are complimentary to ours. We attract the most talented employees by providing a highly competitive compensation package, and we seek to retain them by fostering a work environment in which employees can thrive professionally and personally.