Information Security as a Service (ISaaS)

The Future of Information Security

by Kevin D. Murray, CPP, CISM, CFE, CDPSE

Free-world businesses know they have a problem. They are bleeding their life-blood. Manufacturing was phlebotomized first. Bleeding now is the intellectual property and confidential information. What happens when these are gone?

We are watching a death of a thousand cuts, but it can be stopped. This paper examines how to do it.

IT departments are in the spotlight as the protectors of information. Yet, they can't keep up with hack attacks, info-theft, ransomeware, and leaks. They are playing a grown-up version of whack-a-mole. Their valiant efforts are not enough, and they know it.

IT Cries for Help

The one word we keep hearing from IT is ***overwhelmed***. It is in the news practically every day…

- As IBM's Security Intelligence underlines, security analysts are overworked, understaffed and overwhelmed.[1]
- Many teams are missing the attacks that significantly impact organizations because they don't have the size or expertise to keep up with the attackers and are overwhelmed.[2]
- …it's easy to get overwhelmed[3] by the number of online threats posing real risk to your business…
- General purpose IT managers are valuable, but they can also be overwhelmed[4] with every technical issue that comes up in a less-than-technical organization.
- …traditional IT security mechanisms are easily overwhelmed,[5] and unprotected companies risk serious business disruption, loss of revenue and even fines.
- The sheer number of cyber threats can seem overwhelming,[6] even for businesses with large IT departments.

But what usually goes unreported is the related costs to an organization of having to chase alerts day in and day out. Those costs take a human toll and a business toll and can be measured in lost time, lost employees, and lost money.[7]

Not Just an IT Problem

Most computer-related hacks need to be preceded by old school spy tricks:

- pre-attack intelligence collection,
- social engineering and scamming,
- dumpster diving,
- break and entry,
- or a bribe.[8]

Problem 1: Weak security attracts predators. IT security is often an add-on or out-sourced duty at small to mid-sized organizations.

Problem 2: Computers and networks are not the only info-veins being tapped. Even when corporate IT is practiced as a full-time specialty, overall information security can be

[1] https://techerati.com/features-hub/opinions/cyber-security-artificial-intelligence-ai-humans/

[2] https://www.techrepublic.com/article/employees-are-almost-as-dangerous-to-business-security-as-hackers-and-cybercriminals/

[3] https://chiefexecutive.net/avoid-these-top-four-cybersecurity-mistakes/

[4] https://www.rapidgrowthmedia.com/features/UIX_cyber_security_06202019.aspx

[5] https://www.forbes.com/sites/jasonbloomberg/2019/02/12/are-hackers-winning-the-denial-of-service-wars/#6c68041528ea

[6] https://securitybrief.eu/story/why-cyber-threats-are-draining-your-resources

[7] https://www.ci.security/resources/news/article/the-hidden-costs-of-chasing-cybersecurity-alerts

[8] https://www.sailpoint.com/news/market-pulse-survey-2016/

crippled. This happens when security budgets are *too* IT focused.

The Employee Factor

One survey[9] revealed, **"One in five employees said they would sell their passwords… and 44% would do so for less than $1,000"** Yikes!

It was revealed, for example, AT&T employees took bribes to unlock millions of smartphones, and to install malware and unauthorized hardware on the company's network,[10] according to the Department of Justice… The DOJ charged the two with **paying more than $1 million in bribes**… The two suspects recruited AT&T employees by approaching them in private via telephone or Facebook messages. Employees who agreed, received lists of IMEI phone codes which they had to unlock for sums of money. The bribery scheme lasted several years.

Scott Adams understood the problem…

- Stressed employees thinking, *"I have enough to do without…"*
- No one has the authority, or talent, to implement a holistic solution.

Real information security requires multiple talents, working as a team, full-time, to protect information and intellectual assets. Few organizations have this capability. Even fewer understand that a holistic approach is required.

Downward Spirals

Underfunded security budgets weighted toward tangible assets obviously don't work very well. Similarly, underfunded IT budgets rarely work as expected.

Underfunding leaves these critical personnel frantically running a Möbius loop strategy. Aside from not getting anywhere, it is exhausting and discouraging. Exhausted and discouraged people don't perform well.

I'VE BEEN ASKED TO BRIEF EVERYBODY ON THE COMPANY'S POLICY FOR PROTECTING SECRET INFORMATION
ALL SECRET INFORMATION MUST BE LOCKED UP AT NIGHT.
OUR SECRETS COULD BE OF GREAT VALUE TO OUR COMPETITORS.
IN FACT, SOME COMPANIES TRY TO BUY THE SECRETS OF THEIR COMPETITORS.
JUST OUT OF CURIOSITY HOW MUCH WOULD OUR COMPETITORS PAY FOR OUR SECRETS?
OH, I DUNNO . . . MAYBE SEVERAL TIMES YOUR ANNUAL SALARY.
I DON'T THINK THIS WAS SOME OF MY BEST WORK.

Why Are Organizations So Poor at Protecting Themselves from Information Theft?

Several reasons…

- Employee leaks (accidental, or on purpose)
- Internal knowledge and responsibilities are too compartmentalized.
- Crossing job boundaries is politically risky.

Information protection negligence creates a spiral of doom.

1. Losses go undetected.
2. Undetected losses can't be calculated.
3. Without accurate calculations new budgets are inaccurately low.
4. Low budgets make information theft easier.
5. Easy targets get hit more often.
6. Eventually the organization is info-sucked dry.

[9] https://www.businesswire.com/news/home/20160320005022/en/SailPoint-Survey-1-in-4-Employees-Will-Share-Sensitive-Information-Outside-the-Company

[10] https://www.zdnet.com/article/at-t-employees-took-bribes-to-plant-malware-on-the-companys-network/

Fluid Things Leak

Information is fluid. It is generated, transmitted and stored. **Every** step of its journey requires protection. Protection is not solely an IT responsibility. They are last in the line of easy targets. Remember, almost everything stored digitally was available for theft elsewhere *before* it became data.

The information journey begins with the spoken word. Ideas, strategies, proposals all begin with discussions. This is the freshest and thus the most valuable information an adversary can appropriate. Attacks against words, thoughts and strategy plans include: electronic surveillance (room bugs, taps, communications spyware, etc.), social engineering, infiltration, bribes and blackmail.

Information's journey continues as these thoughts, words and collected data are documented, transmitted, and ultimately stored. Each stage of the process requires a unique set of protections. Clamp security on just one area and, like a water balloon, the other areas instantly become more vulnerable and attractive targets.

Fluid information leaks in many ways:

- paperwork left on desktops,
- inherent office equipment vulnerabilities,
- whiteboards facing windows,
- unlocked filing cabinets,
- employee discussions in public venues like restaurants and conference centers,
- ineffective access control,
- decaying security hardware,
- sensitive wastepaper disposed improperly,[11]
- sensitive areas bugged[12] with surveillance devices,
- employees not following security policies,
- disloyal employees,[13]
- and even blackmail[14] of "loyal" employees.

Competitive intelligence involves collecting bits of information, in many different ways. Sometimes a big picture can be divined by competitors even before the target company has solidified its own plans.

The Solution — Information Security as a Service (ISaaS)

The future of information security is not in the hands of:

- IT departments,
- Security departments,
- Technical Surveillance Countermeasures (TSCM) techs,
- policy scribes,
- security systems designers,
- or, the security educators who train employees.

The future of information security is in the hands of the savvy organization, security service, or consulting firm that can synergistically orchestrate *all of the above* talents.

Think of this approach like the doors and windows at a bank. **All** need to work in unison to protect the riches within.

Rules of Thumb

1. *"There is good information security,*
   there is cheap information security,
   but there is no good cheap information security."
2. The greater the information's value, the more expensive the lock should be.
3. The key to successful information security is a holistic approach.

The In-House Solution

A holistic information security program has a chance of succeeding in enterprise organizations if they dedicate the money and talent to support it internally.

[11] https://counterespionage.com/shred-bin-security/

[12] https://www.foodnavigator-usa.com/Article/2011/11/15/The-tip-of-the-spyberg-Is-your-boardroom-bugged

[13] https://www.workforce.com/news/keep-spies-out-of-your-company

[14] https://www.npr.org/sections/parallels/2017/04/11/523416914/russian-spies-go-to-tactics-for-entangling-people-bribery-and-blackmail

The biggest benefits of the in-house solution are instant response and accountability. So why is this implemented at so few companies?

There are a few challenges to overcome…

- Compliancy.
- Corporate culture.
- Short term profit goals.
- No one wants to take on extra work.
- Reliance on faulty risk assessments due to information loss being hard to quantify.

If parsimonious describes your organization's management, you're doomed. Protecting critical information requires commitment, and an investment.

What about all the organizations that are not supporting a full-time effort? How will they achieve a successful information security posture? Who can they call for help?

The Best Information Security Solution for All Concerned

Consider this…

- IT consultants only help with IT issues.
- Technical Surveillance Countermeasures (TSCM) techs just check for room bugs.
- The alarm folks push hardware solutions.
- Guards aren't trained to spot information security vulnerabilities.
- Employees without policies to follow and proper training are weak links.
- Insider threat behavioral scientists focus their talents on people alone.

Yet, each one of these (uncoordinated) functions is a necessary brick in the information security wall.

An Information Security service specializing in a holistic approach is the answer. They can standardize and orchestrate the important essentials.

A "shut all the doors and windows" ISaaS approach would address: (Not a complete list, and in no particular order.)

- Information Security Policies and Procedures (about personnel, audio, visual and data)
- Information Security Paperwork (Non-Disclosures, Employee Agreements, etc.)
- Employee Information Security Responsibilities
- Insider Threat Behavioral Analysis
- Perimeter Security & Access Control
- Red Team Penetration Testing
- Employee Awareness & Training
- Social Engineering Prevention
- Social Media Monitoring & Management
- Communications Security
- IT and Network Security
- Office Equipment Vulnerability Evaluations
- Technical Surveillance Countermeasures (TSCM) Inspections[15]
- Wi-Fi Security and Compliance Audits[16]
- Off-hours Information Security Surveys
- Security Hardware Assessment
- Security Enhancement Recommendations

This task list may seem overwhelming at first. It's not. A knowledgeable information security specialist can coordinate them. The result will be each stage building upon the previous stage for maximum effectiveness.

From a client's point-of-view… no muss, no fuss, no work, no bother. Just call in ***The Team*** and all will be well.

A simplified ISaaS offering might look like this…

- A baseline vulnerability assessment.
- Establish or enhance information security policies.
- Educational programs for employees.
- Establish a pro-active due diligence schedule for IT, TSCM and physical security assessments.
- Create service alliances with specialized security consultants.

[15] https://counterespionage.com/advanced-tscm-explained/scheduled-tscm-inspections/

[16] https://counterespionage.com/tscm-technology/wi-fi-security-audits/

Who Will Build an ISaaS?

The Future of Information Security is about to arrive. All the elements for ISaaS are here today. It is just a question of who has the foresight to bring them under one roof, before the competition does.

Current businesses already well-positioned to do this include…

- Major contract security providers.
- IT companies providing multifaceted services to businesses.
- Consulting firms offering business strategy, digital, technology and operations services.

Reasons why these well-positioned companies should offer ISaaS to their clients…

- To provide a needed service to a very large marketplace.
- Promote services they already offer.
- Develop their own additional services related to ISaaS.
- The industry prestige associated with forward thinking and being the first.
- ISaaS creates a unique competitive advantage over static competitors.
- A profitable new menu item is always a good thing.

Who can help you create an ISaaS Department?

- I thought you would never ask. Give me a call. I have a few more ideas.

——-

Kevin D. Murray, CPP, CISM, CFE, CDPSE is a business counterespionage consultant and TSCM specialist with over four decades of experience.

Murray Associates is an independent security consulting firm, providing eavesdropping detection and information security services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.