Cooperative Systems
forward thinking IT

Security Program or "Security Theater": 10 Practical Tips to Enterprise-Level Security

This whitepaper addresses key business lessons worth considering when shifting from a "Security Theater" to a more secure organization.

NOAH
information technology services

80 Lamberton Rd., Windsor, CT 06095 • 860.523.1000
67 South Bedford St., Suite 400 West, Burlington, MA 01803 • 781.496.3075
noahsales@coopsys.com
www.coopsys.com

We see this all the time in Cyber Security: Upon entering an organization's IT center you can hear the ringing of phones, the pinging of computers and hardware systems echoing notifications, and the quick steps of IT personnel moving from chair to chair and screen to screen. It looks like the scene out of every air traffic control scene in the movies. There is just one mission and that is to protect innocent lives, ensuring passenger safety and enforcing security. This mission is what drives the actions of each team member and so long as each person believes this will be enough, the world for that day will be safe.

While this scene waxes poetic in movies, it doesn't translate well into the Network or Security Operations Center; none-the-less, much of how security is sold, implemented and managed in the real world is based on the same idealistic, box-office imagery. Underlying much of the security industry is a mindset of fear and the premise of "saving the day." While fear is natural, it can at times become a justification for irrational thinking, unnecessary security spending and more "security theater" than real security.

"Security Theater" is defined by Wikipedia as "the practice of investing in countermeasures intended to provide the feeling of improved security while doing little or nothing to actually achieve it." While making security investments is imperative to any security program, most IT executives have little time to examine the motives behind their security decisions; therefore, some are unaware of the risk they can pose to their own organizations. If the goal is for a company to actually be secure, then it is critical prior to a breach for decision makers and those tasked with managing security to gain greater insight into how and why security decisions are being made. The challenge is to answer, as an organization, the following question: Is our current security program really securing us and does it make us feel more secure? A top-notch security program should strive to address both the need for real security and the desire to feel secure.

Do you recall the "Viper" car alarm commercials of the 90's? It showed a car being broken into by a burglar with a mask. Upon touching the door, a loud robotic voice could loudly be heard stating "Protected by Viper! Stand back!" In the commercial, that seemed enough to catch the burglar's attention, as well as the attention of the television audience. The car was safe again; however, I'm not sure how happy stray cats and little old ladies might feel by mistakenly brushing up against the car. Further, I am not sure there was much more protection that the car's owner received from Viper. Arguably some might argue that "Viper" was "Security Theater" in that it made the car's owner feel safe while providing little actual security. Others might suggest that the voice alone was enough of a deterrent to make this car unappealing to burglars. I would argue that security in this situation may've required Viper in addition to further measures to protect that asset. The lesson here is that feeling secure and being secure are not the same.

We recognize that this topic is a dicey one. It requires that IT executives question their default behavior and act in opposition to the nature of the world in which they operate. What if the truth is that the ISO is not inherently adept at making rational security decisions, especially when presented with ancillary information designed to persuade one way or another?

The ISO of any organization is challenged in five key ways:

- Security companies are designed to create technologies that exploit FUD (fear, uncertainty and doubt) for gain
- Security experts tend to overemphasize military tactics and battle plans over business goals and financial projections

- Every week there is a news story publicizing another breach of a large corporation over the more frequent breaches of smaller companies
- Daily trade-offs and priorities must be set about how to spend limited security budget
- The illusory nature and myths of the Unknown Hacker.

This is the real world as it exists for the ISO today. It is therefore the world in which security programs must be measured and assessed. The hope is that by taking a more practical approach to how our brains process risk, and the biases we use to think about security, we can learn how to embrace our natural tendencies and create security programs with better knowledge overall and less driven by fear. Perhaps we can even learn how to recognize Security Theater, and establish thought leadership among peers on its difference from real security. Organizations such as The Bank of England are even hiring behavioral psychologist for their security teams.

In the article *The Psychology of Security (Part 1)* Bruce Schneier states that, “Security is both a feeling and a reality. And they're not the same. Or, more generally, you can be secure even though you don't feel secure. And you can feel secure even though you're not. The feeling and reality of security are certainly related to each other, but they're just as certainly not the same as each other. We'd probably be better off if we had two different words for them.”

Schneier goes on to say that “the reality of security is mathematical, based on the probability of different risks and the effectiveness of different countermeasures. We can calculate how secure your home is from burglary, based on such factors as the crime rate in the neighborhood you live in and your door-locking habits.” The belief expressed here is that we should design security systems that take the feeling of security into account rather than ignoring it. There's no such thing as absolute security, and any gain in security always involves some sort of trade-off. So, maybe the better question is this: For real security, what tradeoffs are we willing to make?

Here are 5 practical business lessons for moving from “Security Theater” to a more secure organization:

1. **The reality of security is mathematical, based on the probability of different risks and the effectiveness of different countermeasures.**
   Take time to gain more quantitative and directly relevant data on: The current state of your technology program, what works and isn’t working, how much budget you have to spend today and in the future, what your goals are for improving security and how to effectively reach your goals.

2. **Security is also a feeling based on your psychological reactions to both risks and countermeasures.** Do any of these reactions sound familiar? If so, you’re not alone. In *Beyond Fear*, Scheiner lists five major psychological responses to risk:

   i. People exaggerate spectacular but rare risks and downplay common risks.

   ii. People have trouble estimating risks for anything not exactly like their normal situation.

   iii. Personified risks are perceived to be greater than anonymous risks.

iv. People underestimate risks they willingly take and overestimate risks in situations they can't control.

v. People overestimate risks that are being talked about and remain an object of public scrutiny.

3. **You want the organization to BE secure and Senior Management, Users and Customers want to FEEL secure.** You are responsible for both. Often, when the perception of security doesn't match the reality of security, it's because the perception of the risk doesn't match the reality of the risk.

    a. Learn the often complex business art of “Security Perception Management” – People tend to worry about the wrong things: paying too much attention to minor risks and not enough attention to major ones. A lot of this can be chalked up to bad information but there are some general pathologies that come up over and over again. The better you address them, the more likely you can persuade them to make decisions that truly align with your organization’s security needs.

    b. Learn what keeps your organization’s leaders up at night and address those fears first. Have conversations with them early and often to check their temperature and assure them you have a game plan you are putting into action.

    c. Listen to what they say in a room full of people vs to a trusted few. Evaluate their actions against their words. Then take that into account when presenting your solution and gaining approval.

    d. People are more likely to agree with evidence that supports a previously held position than one that challenges it. Going into a meeting and telling the Leadership that if the security budget isn’t raised, the company is in imminent risk of breach, isn’t effective. Most won’t believe you and you will be perceived as irrational and hysterical.

    e. If you want your boss to approve your expensive security budget, you'll have a much better chance of getting that approval if you give him a choice among three security plans—outlining options for three different budgets. Instead of saying I need $1M or else, offer three viable plans of $500K, $1M, and $2M, respectively—with the most reasonable choice being the $1M budget.

4. **Security is a business decision, which involves tradeoffs**. There's no such thing as absolute security, and any gain in security always involves some sort of trade-off. Be prepared to lose something.

    a. Determine in your organization, given the nature of the threats today and your resources, what is the most practical cyber strategy? What are my customers and bosses willing to give up in order to be more secure? Not what should they give up, but what will they give up? Then, start building your security program there.

b. Understand the risks the organization is willing to take.

c. Frame Security in the language of business risk. Remember you are talking to non-security professionals, discuss ROI, value, price and metrics as much as possible using security and relevant financial data

d. In business, convenience and transparency beat Security every time – until there's a breach. This is the truth. Build your Security around this fact, and other, fundamental truths.

5. **The Unknown tradeoffs tend to hurt you more than the known tradeoffs.** Work to learn as much you can about assumptions being made, risks being ignored and anticipate future risks to come.

    a. Without proper data, there is a natural tendency to overestimate on one side of the tradeoff and underestimate on another.

        i. Pay close attention to the following risk indicators

            1. The severity of the risk.

            2. The probability of the risk.

            3. The magnitude of the costs.

            4. How effective the controls and countermeasures are at mitigating the risk.

            5. How well risks and costs can be compared.

6. **To Thine Own Self Be True:** What is your core risk and security philosophy? What are the gaps in your knowledge? What items keep you up at night?

    a. Evaluate your own thinking - If you assume that a risk is greater than it really is, you're going to overspend on mitigating that risk. If you think a risk is real but only affects other people--for whatever reason--you're going to underspend. If you overestimate the costs of a countermeasure, you're less likely to apply it when you should, and if you overestimate how effective a countermeasure is, you're more likely to apply it when you shouldn't. If you incorrectly evaluate the trade-off, you won't accurately balance the costs and benefits.

7. **Security costs money, but it also costs in time, convenience, capabilities, liberties, and so on.** Take each of those into consideration when building your program. If a vendor tell you it's "plug and play" or does the most of the work by itself – show them the door. No matter how much you spend on a next-gen or managed firewall, unless you dedicate an adequate amount of time, resources and additional funding to tuning and reducing the noise, you've added more "security theater".

8. **Assume you've been asking the wrong questions about your security all along and begin asking vendors the right ones**. It makes no sense to just look at security in terms of effectiveness.

"Is this effective against the threat?" is the wrong question to ask. You need to ask: Is it a good trade-off for our company, at this time and based on our needs.

9. **Get Consensus Early and Often**: evaluating security decisions as a group makes them feel less risky than evaluating them one at a time. Communicate, Communicate, Communicate – up, down and across the organization. Seek feedback, learn more about internal and external customer security and IT wants, desires, concerns and build them into your roadmap.

10. **Build trusted partnerships, not vendor relationships.** Security Programs demand ongoing management and monitoring. It takes more than a tool and a dream. Find a trusted security provider who will work with you to build a roadmap to real security and understands your specific budget and vision.

    a. Nervous about third parties? Many companies share this concern. Often, security is equated with control. The assumption is that since an employee's organization is typically most knowledgeable about details of its own systems, it is best suited to mount a defense to protect itself. Therefore, the more control it can exercise on its perimeter by keeping threats out and data in, the more likely it could effectively risk reduce its security risk. As a result, many companies spend thousands, even millions, on building internal security programs with staff, firewalls, DLP and SIEM's in an attempt to "secure its walls." There is some value to this line of thinking. But, much of the data today disputes this approach. Building a mature security program requires an organization to align with a strategic security partner – one that aligns closely with its philosophies and augments its own people, processes and technologies. A trusted security partner provides three major benefits:

    b. Expands the diversity of skillsets you currently have in-house. Securing an enterprise takes the work of security analysts, engineers, project managers, incident response managers, vulnerability managers and a security expert who can effectively provide guidance on the latest threats, industry trends, new technologies and research how they fit into your current program.

Today, there is an invisible line between "Security Theater" and real security. Success in Security Leadership demands that the ongoing roadmap include efforts to build the core technical components of a highly resilient security program and address the natural desire of business leaders to actually feel secure. The latter function requires some business acumen and "soft skills" related to active listening, effective communication, presentation skills, collaboration and empathy with internal and external customers. In other words, a solid enterprise security program demands a Ying & Yang approach, which combines sheer technical power with an ability to bring harmony through communication and engagement across the organization. Both are critical, but having heard the complaints of CISO's following a large data breach, managing the risk discussion and communicating them to relevant parties are more important than implementing the best technology available.

Cooperative Systems has provided Information Technology solutions to the SMB market since 1993 when it was established. Our relationships with partners such as Microsoft, HP, Dell, VMware, and Cisco have allowed us the ability to design, scale and implement effective infrastructure solutions for our diverse client base. Our Solution Stack includes custom designed Cyber Security Solutions, Voice over IP (VOIP) Solutions and Phone Systems, Structured Voice and Data Cabling, Mobile and Wireless, Physical Security Solutions, Website Design, Local and Wide-Area Networking, as well as Managed Services. As a Certified Microsoft Partner, our Core Competencies include Server Administration, Networking Infrastructure, and Managed Services Solutions.

We specialize in educating you in the Information Technology options available to ease your business' IT concerns in the 21st century. Our professional scope ranges from engineering and implementing Telecommunications Systems and Local and Wide Area Networking Solutions, to architecting and designing custom Voice and Data Cabling Solutions to address your specific business needs. Cooperative Systems Network and Technical Engineers' combined experience allow us the ability to successfully provide custom, affordable solutions to our valued Clients.

Our technical expertise enables us to provide Network Design and Support, as well as Communication Design for Office Automation, and Structured Voice and Data Design; utilizing technologies such as Broadband Internet, Dedicated Connectivity, Point-To-Point Tunneling Protocol, and Virtual Private Networking. These technologies provide the ability to securely design and structure your equipment, optimizing communication, productivity and overall business progress.

By coordinating and managing all of your technical solutions and Vendors, and proactively managing your network, you would see the benefits of the ability to completely focus on running your organization.