



www.burnsmcd.com

SECURITY COMPLACENCY: THE THREAT OF DOING MORE WITH LESS

AUTHOR:

Stephen A. Brown, CPP, CHS
Director, Global Security Services, Burns & McDonnell

Kotter’s first source of complacency, notably, is the absence of a major and visible crisis — simply stated, security complacency. The bottom line is this: Can you afford security complacency in today’s work environment, even in these tough economic times? The answer is no.

CONCLUSION

So what should you do? First and foremost, develop a thorough understanding of the threats, risks and vulnerabilities your organization faces. While there may be known threats in your city or region, these threats may or may not be directed at the products or services you provide. Even if all known threats are directed away from you, it does not mean you can ignore them, particularly if the threats target your neighboring businesses.

Second, be certain your integrated security systems are working as designed. Are your cameras monitoring your critical assets? Are your DVRs recording continuously or only when an alert is sounded? Are your intrusion detection sensors working as planned or are they covered with dust?

Third, evaluate your security policies and procedures relative to the current threats and risks your organization faces. Are your security operations manuals, post orders, flow charts and other resources current? When was the last time you tested your incident response plans? Do your key

personnel know what is expected of them, especially in light of changing roles for many staff members as the economy softens?

Finally, determine if your employee security awareness training has taken a backseat. Your employees can see and hear far more than any integrated security system, and, more importantly, they can and will bring security concerns to management’s attention if trained and asked to do so. Employee security awareness training is a critical step for all corporations and public organizations.

In an economic downturn, doing more with less is a necessity; however, it also poses a threat to security. That is a risk not worth taking, as it could create vulnerabilities in these uncertain times.

IN AN ECONOMIC
DOWNTURN, DOING MORE
WITH LESS IS A NECESSITY;
HOWEVER, IT ALSO POSES
A THREAT TO SECURITY.

In today’s tough economic times, the business principle of doing more with less is at the forefront for most corporations and public organizations. Executives to mid-level managers are being tasked with thoroughly examining their budgets and finding ways to cut back. Far too often, the reduction in funding comes at the expense of security staffing and initiatives. We have come to learn that when security is cut back, complacency sets in, and the secure feeling we once enjoyed gives way to potential risks and vulnerabilities.

Complacency is defined by Merriam-Webster as “self-satisfaction, especially when accompanied by unawareness of actual dangers or deficiencies.” This protection clearly defines why we cannot accept complacency when it comes to security.

When we reduce security, we become more susceptible to higher incident costs and harm, which are contrary to the goal of austerity.

This past decade has seen a roller coaster of activity in the security arena, and the decisions we are now making, as well as those we will make in the next few years, will greatly impact our security posture and set the standard for years to come.

WHERE IT BEGAN

Our nation’s security posture changed on Sept. 11, 2001. Private-sector corporations and public organizations quickly realized their security policies and procedures, as well as their business continuity plans, were inadequate in the face of such a catastrophic event.



The initial response: Increase funding to remedy the situation. Not just a few dollars, but hundreds of millions of dollars, making the United States one of the most secure countries in the world — if not the most secure — by the end of 2005.

LOOKING BACK

Of the three biggest security incidents of the 1990s — the first World Trade Center bombing, the Murrah Federal building bombing in Oklahoma City and the Columbine High School shooting — two came from within our borders. Unfortunately, that promoted an overall comfort level for most residents, and physical security concerns did not become a priority.

But questions surfaced on that sunny Tuesday morning in the fall of 2001 when our world changed. Everyone — employees, employers, family, friends, law enforcement, firefighters and other first responders — had a story about not being able to make contact with someone. Everyone wanted to know how such a massive terrorist attack could occur on U.S. soil. There were no solid answers, but experts said to expect a similar incident if enhanced security measures were not implemented.

Over the next four years, integrated security systems business boomed. Organizations installed high-tech, expensive cameras with digital recording systems business boomed. Card access systems required everyone to display their credentials. Intrusion detection systems became the guardians of windows

and roof openings. World-class security operations centers were staffed with guard forces. These steps were a necessary good start.

CHANGE OVER TIME

However, in the latter half of this decade, the economy turned south. Corporations and public organizations struggled, and many reduced their workforces. Security became one of the first areas facing cutbacks. Most organizations felt confident the security systems in place would provide the necessary coverage and protection. But as security directors were asked to do more with less, security operations centers experienced reduced staffing and guard force hours. Employees quickly learned their actions were no longer monitored, and many became lax in following security procedures. Maintaining employment took priority over seemingly minor security procedures.

When employee security procedure enforcement waned, the integrated security systems followed close behind. Tailgating — a method of entering secure buildings by following closely behind the person ahead without swiping another access badge — became second nature, rendering card access systems worthless. Operational changes mean no one monitors the high-tech cameras that watch our critical assets. Intrusion detection systems have become ineffective because few staff members are available to monitor them or test system operation.

A NEW THREAT

Lax security procedures leave many exposed to varied threats, from the less probable terrorist attack to the most common threat of all: workplace violence. In today's economic downturn, this threat affects every organization as layoffs increase, which places additional stress on the remaining workforce, as they are also asked to do more with less.

According to the U.S. Bureau of Labor Statistics, assaults and violent acts account for 16 percent of workplace deaths, second only to fatal transportation incidents. Workplace violence is the leading cause of death among women in the workplace. While annual fire drills are common, most organizations fail to prepare for an incident of workplace violence, a threat that increases as the economy declines and security complacency continues.

WHERE ARE WE NOW?

Whether your organization enjoys continued success or is one of the many that have cut security budgets, it is important to thoroughly assess your integrated security systems and current security measures. The expense of gaining first-hand knowledge of your current security posture and mitigating identified vulnerabilities will be far less than the cost of mitigating or litigating the results of an attack.

Proven protection strategies of deter, detect, deny, delay and respond can be implemented with low-cost initiatives, especially when integrated security systems

are already in place. A thorough review of security policies, procedures, post orders (shift-specific duties) for security officers and incident flow charts can identify areas that need immediate attention.

While society deems it polite to hold doors for strangers with their hands full, the reality of the security landscape requires us to be more aware. A policy regarding visual display of credentials helps, but only if employees are trained to request it when identification is not obvious and follow through until it is provided. John Kotter, author of *Leading Change*, identifies nine sources of complacency:

- No significant crisis
- Abundant, easily accessible resources
- Insufficient performance expectations
- Lack of emphasis on working for the greater good
- Focus placed on too narrow or wrong goals
- Lack of third-party feedback
- Unwillingness to address weaknesses
- Propensity to deny problems exist
- Overstating success and down-playing challenges

ASSAULTS AND VIOLENT ACTS
ARE THE SECOND-LEADING
CAUSE OF WORKPLACE DEATHS.
