MINIMIZING YOUR VULNERABILITY pdf

1: Reducing Risk Through Effective Vulnerability Management

Newborn security: Steps toward minimizing your vulnerability. Ensuring that Mom can recognize her own baby is a good first step. Your procedures and policies on infant security warrant an especially close look in light of the notorious "baby switch" that's currently plaguing quality colleagues at the University of Virginia Medical Center in Charlottesville.

February 28th, With 23 years of IT experience â€” including 10 related to financial services â€” Ed Bilewicz, currently vice-president of application hosting for Solutions Inc. He shares with IT Focus the lessons he has learned along the way. What are the data centre management outsourcing choices facing financial services companies today? There are basically three kinds of models in a hosting scenario. Then the other end of the spectrum is the model that I currently favour and use which is called co-location co-lo. You give me the power, the fire suppression. You give me the bandwidth into the Internet. But I will manage everything else. I need to get it mounted up in cabinets, need power drawn to it and connected to the network. So you would be selecting, purchasing, implementing, installing the hardware and software? Right, and then I just plug into their router to get out onto the general Internet. Then in the middle is kind of a hybrid thing. Then I let them manage the backup. I just tell them when I want it, when I need it. There are a lot of products out there that monitor infrastructure health. A lot of these services are non-intrusive. I had to get up and running quick. So we started almost as a fully managed service. So if I needed to go outside that service for a bit, or I needed to tweak it a little bit, then it would have been a custom solution and would have cost lots of money. Can you give me an example? We had a fully managed firewall service here. The way the normal Internet data works is that you just need your outer secure zone open to the whole world. So we have to shut down and only allow in specific carrier gateways. In that case, you have to do a change quickly. With fully managed service, you can get a hour turnaround. Well, we needed to do it immediately, so we needed the service level that was immediate. Over time we migrated here to co-lo where we run everything ourselves and they just give us space. We run back-ups, restores, troubleshooting, install the applications, install the operating systems â€” all that stuff we do from up here. So when is going with managed services advisable? They understand better the web hosting and the wireless side of things. Plus a lot of the enterprise customers are comfortable with the big name companies. When would one steer away from fully managed outsourcing? Once you do have staff, you can probably do things faster in co-lo. Usually in a fully managed service you fall into a more traditional project implementation. We need this environment built here â€” go out and do it, then come back and build the next one. Moving from a fully managed service provider is a much more contemplated exercise. The other thing co-lo lets me do is I can bring stuff up quicker. I want this, this, this and this. But what if your provider closes? If I use any of their managed services, I have to get the same thing somewhere else â€" and nobody does everything exactly the same. So the way I would set up an environment is, I would take provider A and provider B and I would go co-lo. I would not use any of the managed services as long as I have the mandate to get staff. The mandate to get staff allows me to put a management or operations layer above it all. I can still offer a consistent service. How do you know that you have to move quickly? You just assume you have to move quickly. If you can afford it you should go with two providers â€" different companies â€" and then you should start distributing your customers across both. We alternate; we crisscross the two. The QA environment is essentially a close approximation of the production environment. Then we cross populate into environments. When I back up this production environment at one provider , that backup gets stored over at the other provider so that if one provider takes a hit I invoke disaster recovery, and I just bring up their QA environment as the production environment until I can scramble and get another QA environment for them somewhere else. So they have no loss, minimal downtime, or no interruption of the services. What that allows me to do is distribute my risk. What other lessons have you learned? You want to avoid the pure co-lo providers. Another lesson we learned is if you need flexibility in the service, then you have to bring it in house. What is important to look for in a service provider? You want to look for the actual operations to have some kind of a certification designation. There are a couple out there â€" SAS What you want is consistent service from these guys. I would always check out the facility first hand. I would physically go down there. You want to make sure they have generators that are fired and tested regularlyâ€¦. You want to make sure their UPS uninterrupted power supply is there and tested. You want to make sure their air flow is good. You want to check their physical security. You want to make sure their security guys are background checked. How do they do their key controls? You want to make sure that there are mantraps one door shuts before the next open so no one can follow undetected. You want to make sure there are multiple levels of security. You want to make sure you have cameras down every row, every aisleâ€¦ the security guards are checking the cameras. Usually you want to make sure they have to deposit some sort of ID at the front, so they have to come back to pick it up. Usually if one of these guys runs into trouble, there are a few others that get into trouble. You want to look at their client base. You want to look for more traditional companies; what they call enterprise companies, like well-known names. What might they overlook? You need to set the price, then set the expectation. So SLAs are important. But there should be an expectation on how they react or interact with you as well. It should always come through a single authorized contact. You need to have everything documented. You need to be kind of rigorous in that because as soon as your documentation goes out of date, and then if you have to move or do something, it makes it more difficult. We always make sure our DR disaster recovery plans are current and tested in case we have to go to another provider.

2: Newborn security: steps toward minimizing your vulnerability.

As you can see, there are a variety of strategies for reducing vulnerability risk. There's no silver-bullet that will work perfectly across all organizations. While employing the right tools can help, knowing how your organization operates is what will make the difference between an expensive product and an effective program.

Jason will also provide participants with a practical, five-step approach to restore trust in your critical systems after a data breach. Register today to join us for this informative webcast. Michael will also provide participants with a practical, five-step approach to restore trust in your critical systems after a data breach. Which systems can be trusted? What is the extent of the compromise? How quickly can you attain situational awareness? He will also provide participants with an approach to restore trust in your critical systems after a data breach, following five steps: Know what you have and prioritize by risk levels 2. Harvest system state information from your production systems 4. Perform a reference node variance analysis to identify compromised systems 5. Remove suspect systems from the environment and return to a trustworthy state Join us for this informative webcast! Advice from the QSA Recorded: Jan 22 57 mins Adrian Sanabria As a former QSA and currently a security analyst at The Research, Adrian Sanabria will share a frank viewpoint of how the new version of Payment Card Industry standard will affect your organization. Join us for this webcast and you will: Tune in to hear: How to Prioritize and Respond to Risk Recorded: Oct 4 36 mins Gavin Millard Please accept our apologies for the technical difficulties encountered with this webinar on Monday. This is now due to take place on Friday 4th October. Go Beyond Scanning Recorded: In this webinar, you will learn:

3: 5 Strategies to Reduce Stress and Emotional Vulnerability | The Oz Blog

1. Hosp Peer Rev. Oct;23(10) Newborn security: steps toward minimizing your vulnerability. [No authors listed] PMID: [PubMed - indexed for MEDLINE].

Additional Resources All facilities face a certain level of risk associated with various threats. These threats may be the result of natural events , accidents , or intentional acts to cause harm. Regardless of the nature of the threat, facility owners have a responsibility to limit or manage risks from these threats to the extent possible. An Interagency Security Committee Standard which states, "Risk is a function of the values of threat, consequence, and vulnerability. The objective of risk management is to create a level of protection that mitigates vulnerabilities to threats and the potential consequences, thereby reducing risk to an acceptable level. A variety of mathematical models are available to calculate risk and to illustrate the impact of increasing protective measures on the risk equation. Threat Assessment Figure 1. A threat assessment considers the full spectrum of threats i. The ISC standard only addresses man-made threats, but individual agencies are free to expand upon the threats they consider. The assessment should examine supporting information to evaluate the relative likelihood of occurrence for each threat. For natural threats, historical data concerning frequency of occurrence for given natural disasters such as tornadoes, hurricanes, floods, fire, or earthquakes can be used to determine the credibility of the given threat. For criminal threats, the crime rates in the surrounding area provide a good indicator of the type of criminal activity that may threaten the facility. For example, a facility that utilizes heavy industrial machinery will be at higher risk for serious or life-threatening job related accidents than a typical office building. For terrorist threats, the attractiveness of the facility as a target is a primary consideration. In addition, the type of terrorist act may vary based on the potential adversary and the method of attack most likely to be successful for a given scenario. For example, a terrorist wishing to strike against the federal government may be more likely to attack a large federal building than to attack a multi-tenant office building containing a large number of commercial tenants and a few government tenants. However, if security at the large federal building makes mounting a successful attack too difficult, the terrorist may be diverted to a nearby facility that may not be as attractive from an occupancy perspective, but has a higher probability of success due to the absence of adequate security. In general, the likelihood of terrorist attacks cannot be quantified statistically since terrorism is, by its very nature random. Specific definitions are important to quantify the level of each threat. The more specific the definition, the more consistent the assessments will be especially if the assessments are being performed by a large number of assessors. Example assessments are provided below: There are aggressors who utilize this tactic who are known to be targeting this facility or the organization. There is a history of this type of activity in the area and this facility is a known target. Specific threats have been received or identified by law enforcement agencies. Events of this nature occur in the immediate vicinity on a frequent basis. There are aggressors who utilize this tactic who are known to target this type of facility. No specific threat has been received or identified by law enforcement agencies. Events of this nature occur in the immediate vicinity periodically i. There are aggressors who utilize this tactic, but they are not known to target this type of facility. There is a history of this type of activity in the area, but this facility has not been a target. Events of this nature occur in the region on a sporadic basis. No aggressors who utilize this tactic are identified for this facility and there is no history of this type of activity at the facility or the neighboring area. There is no history of this type of event in the area. Vulnerability Assessment Once the plausible threats are identified, a vulnerability assessment must be performed. Impact of loss is the degree to which the mission of the agency is impaired by a successful attack from the given threat. A key component of the vulnerability assessment is properly defining the ratings for impact of loss and vulnerability. These definitions may vary greatly from facility to facility. For example, the amount of time that mission capability is impaired is an important part of impact of loss. If the facility being assessed is an Air Route Traffic Control Tower, a downtime of a few minutes may be a serious impact of loss, while for a Social Security office a downtime of a few minutes would be minor. A sample set of definitions for impact of loss is provided below. These definitions are for an organization that generates revenue by serving the public. The entire facility may be closed for a period of up to two weeks and a portion of the facility may be closed for an extended period of time more than one month. Some assets may need to be moved to remote locations to protect them from environmental damage. The facility is temporarily closed or unable to operate, but can continue without an interruption of more than one day. A limited number of assets may be damaged, but the majority of the facility is not affected. The facility experiences no significant impact on operations downtime is less than four hours and there is no loss of major assets. Sample definitions for vulnerability ratings are as follows: The vulnerability assessment may also include detailed analysis of the potential impact of loss from an explosive, chemical or biological attack. Professionals with specific training and experience in these areas are required to perform these detailed analyses. A sample of the type of output that can be generated by a detailed explosive analysis is shown in Figure 2. This graphic representation of the potential damage to a facility from an explosive attack allows a building owner to quickly interpret the results of the analysis. In addition, similar representations can be used to depict the response of an upgraded facility to the same explosive threat. The results of blast assessment depicted in Figure 2 were for glazing only. Existing facility left and upgraded facility right C. Risk Analysis A combination of the impact of loss rating and the vulnerability rating can be used to evaluate the potential risk to the facility from a given threat. A sample risk matrix is depicted in Table 1. High risks are designated by the red cells, moderate risks by the yellow cells, and low risks by the green cells. Matrix identifying levels of risk Minimal Threat.

4: Six Strategies for Reducing Vulnerability Risk

Reducing your vulnerability to virus attacks means you have to take the time to determine how your computer usage and habits might expose you to a computer virus. Several usage habits can have a direct relation on the level of vulnerability of your computer.

More Topics Rings of Protection: How well we protect our assets is up to us. Terrorists can choose from a wide variety of attacks to execute against this country, including kidnapping, murder, cyber, product adulteration, or use of weapons of mass destruction biological, nuclear, incendiary, chemical, or explosive agents. Every business has assets, whether they are people, information, equipment, services, or products. Every asset is vulnerable to attack, and every asset can be protected. How much we spend to protect that asset e. Terrorists the bad guys could target an asset for a number of reasons--it is a piece of critical infrastructure; destruction of the asset will have a significant negative financial impact on a company, a region, the country, or the world; attacking the critical asset is a diversion for another attack elsewhere; or the asset itself can be used as a weapon of mass destruction. The bad guys are not going to expend resources on attacks that are not likely to succeed. The simple reason for this is that terrorism costs money. The bad guys need to invest substantial amounts of time, energy, and money to put an attack together. The terrorists must sell their plan to both their leadership and supporters in order to secure the resources they need. Their three major investment categories are: The bad guys must recruit the operative s to plan and conduct the attack. This person s must be smart, reliable, motivated, and trainable. The training period can be extensive, with significant amounts of time spent not only on executing the attack, but also in preparation recruiting, planning, reconnaissance, logistics, and transportation. Depending on the complexity of the attack, the training period can take weeks, months, or even years. The bad guys will need a laundry list of equipment in order to succeed, everything from transportation to housing, to the weapons needed for the attack. Some of the equipment is legal, cheap, and easy to obtain computers , while other equipment is illegal, more expensive, and takes longer to develop the right relationships in order to obtain weapons of mass destruction. Significant financial resources may be needed to develop and execute an attack. Money will be needed to feed, transport, and house the terrorists and maybe their families ; to provide the training necessary to plan and execute the attack; and to purchase the resources needed to successfully plan, reconnoiter, and execute the attack. The bad guys want to protect their investment. They want the operative to be able to execute the attack and be available for another attack on another day. Therefore, they will not go against our strength or even our perceived strength. What Can We Do? In order to protect our people and facilities, we need to convince the bad guys they do not want to risk expending the resources on an attack that is not likely to succeed. We need to implement rings of protection for our critical assets, whether they are people, infrastructure, economic, equipment, products, or intellectual. The basic criteria for vulnerability to attack are intent, motivation, capability, and ease of attack. If any one element is removed, the chain is broken and vulnerability approaches zero. Clearly, the only leg over which we have direct influence is ease of attack. Remember that the bad guys need the attack to be successful, and they will not go against our strength or even our perceived strength. We must convince the terrorists an attack against our facility would not succeed and therefore would be a poor investment of their resources. Three Ds and an R A well-structured protection plan will have four overlapping and intermixed rings of protection: Rings of protection that are properly deployed will not only provide real security, but also a perception of security that goes beyond the actual improvements installed. The chances for success of dissuading an attack increase greatly and become value added when the rings of protection overlap, and one enhancement will provide value in multiple rings i. Deter--Remember, perception is reality to the bad guys. Every asset is a potential target, so there are plenty of choices to select from and plenty of opportunity to attempt an attack. The best indicator that an asset may be targeted is direct observation or evidence that an asset is or has been under surveillance. Therefore, the goal at this outermost ring of protection is to "scare the bad guys away. We know the bad guys will reconnoiter a target before executing an attack, so if we can scare them away quickly we can interrupt the planning process and avoid being targeted. Examples of deterrents include highly visible and professional-appearing security forces that make frequent, random patrols, as well as man fixed security points; appropriate levels of fencing, lighting, access control, and intrusion detection; and provisions for personal and vehicle inspections, as well as identification and background checks of individuals as one gets closer to the critical asset. Detect--The earlier the planning, reconnaissance, or attack itself is detected and interrupted, the less likely it is to succeed. Optimally, the attack should be detected during the planning or reconnaissance stage by having systems in place to reveal the presence of the bad guy trying to collect intelligence about the critical asset. Training employees about specific activities that should be considered suspicious and how to report this to the appropriate authority would be the outermost level of detection. Background checks and searches are valuable in screening potential employees, contractors, truck drivers, and visitors before they enter the facility. Intrusion detection systems, surveillance cameras, alarms, and frequent, random inspection rounds by security guards make up the innermost level of the detect ring. Delay--If we are unable to deter or detect the bad guy, we must have sufficient physical and administrative barriers in place to make it difficult to gain clear and direct access to the critical asset. We must take the appropriate steps to ensure the bad guys do not have a straight run directly to the target. Typical delaying tactics include remote check-in points; verification of identity and purpose of visits; searching of person, parcels, and vehicles; multiple layers of fencing or other physical blocking devices such as tire shredders and "jersey barriers"; and locked doors with access control systems. Respond--If all else fails, we must have the appropriate capability to respond to the likely consequences of a successful attack. Emergency pre-planning activities must change their focus from the traditional "accidental" damage scenario to the current "on purpose" scenario, whereby someone is intentionally trying to cause the greatest amount of damage and casualties. Local law enforcement agencies must now participate in the pre-emergency planning process to include security issues. Careful review and coordination of both the municipal and private industry joint response capabilities and equipment must be completed, with clearly delineated areas of responsibility. There must be redundant capabilities for communications and mitigation. Pre-emergency planning and periodic emergency exercises with fire, emergency medical services, and law enforcement increase the chances of success. A strong emergency response capability also can serve as a deterrent to an attack if the bad guys believe the consequences will be quickly and successfully mitigated. Conclusion Every asset is a potential target, and every asset can be protected. The bad guys need their attack to be successful and therefore will not go against our perceived strength. Our job is to establish overlapping and intermixed rings that will provide perceived and actual protection against attack. We must revisit our hazard assessments and emergency pre-plans with an eye toward the intentional act and the more severe consequences a successful attack will bring. We must work closely not only with the fire and the emergency medical service, but with law enforcement as well in the planning and execution of emergency exercises. We must partner with the local municipal emergency responders to pool our personnel and equipment to ensure the quickest, most efficient, and safest response in the event of an attack.

5: Minimize your organizationâ€™s threat exposure with Qualys ThreatPROTECT - Help Net Security

Reducing Vulnerability to Negative Emotions: This is a skills that we can use to keep ourselves less vulnerable to having negative emotions, and less likely to get into a state of Emotion Mind, where emotions control our thoughts and actions.

Thus, substance use can trigger a psychiatric disorder and lead to more severe symptoms and other impairments. Because most people with co-occurring mental and substance use disorders have a biological vulnerability to psychiatric disorders, they tend to be highly sensitive to even small amounts of alcohol and drugs. Stress Stress in the environment can worsen biological vulnerability, worsen symptoms, and cause relapses. Stress is anything that challenges a person, requiring some kind of adaptation. Serious stressful events include losing a loved one, getting fired from a job, being a victim of crime, or having conflicts with close people. Stress is often associated with negative events, but positive events and experiences may be stressful as well. For example, performing well in school, getting a new job, starting a new relationship, having a baby, or being a parent all involve some degree of stress. It is also possible for stress to be caused by not having enough to do. When people with co-occurring disorders have nothing purposeful or interesting to do, they tend to have worse symptoms and are more prone to using substances. So a lack of meaningful involvement in life-in areas such as work or parenting, for example-can be another source of stress. Coping Skills Developing coping strategies can help with handling stress and reducing its negative effects on vulnerability. Examples of coping skills include relaxation skills for dealing with stress and tension social skills for connecting with people, dealing with conflict, and getting support coping skills for managing persistent symptoms such as depression, anxiety, and sleeping problems Stress is a normal part of life. Effective coping enables people to be engaged in interesting, rewarding activities that may involve stress, such as working or being a parent. Coping efforts can make it possible for someone with co-occurring disorders to live a normal life without suffering the negative effects of stress. Meaningful activities can include: Supportive people can help in a variety of ways, such as helping people solve challenging Problems supporting people in using coping strategies to deal with symptoms and substance-use urges being open and willing to discussing and resolving personal disagreements, misunderstandings, and areas of conflict that could otherwise lead to stress letting people know that they are important and cared about supporting the person in pursuing personally meaningful goals People who have good social support are less vulnerable to the effects of stress on their psychiatric disorder. Therefore, having strong social support enables people with co-occurring disorders to handle stress more effectively, and live a normal life. Treatment Implications of the Stress-Vulnerability Model Based on an understanding of the stress-vulnerability model, there are many ways to help people manage their psychiatric illness and co-occurring substance use disorder. In the broadest terms, the severity and course of a co-occurring mental health disorder can be improved by reducing biological vulnerability and increasing resiliency against stress. Reducing Biological Vulnerability Biological vulnerability can be reduced in two primary ways: Medication can be a powerful way of reducing biological vulnerability by helping to correct the imbalances in neurotransmitters chemicals in the brain responsible for feelings, thinking, and behavior believed to cause psychiatric disorders. By taking medication, the symptoms of a psychiatric disorder can be lowered and the chances of having a relapse can also be reduced. Avoiding alcohol and drug use can reduce biological vulnerability in two ways. First, because substances affect the brain, using alcohol or drugs can directly worsen those vulnerable parts of the brain associated with psychiatric disorders. Second, using substances can interfere with the corrective effects of medication on vulnerability. This means that somebody who is using alcohol or drugs will not get the full benefit of any prescribed medications for his or her disorder, leading to worse symptoms and a greater chance of relapses. Increasing Resiliency against Stress It is impossible for anyone to live a life that is free of stress.

6: Reduce Vulnerability

The way the normal Internet data works is that you just need your outer secure zone open to the whole world. Banks can't do that because they have restrictions on where you can do transactions.

But you have a lot more control than you might think. Stress management is all about taking charge: No matter how stressful your life seems, there are steps you can take to relieve the pressure and regain control. Why is it so important to manage stress? Stress wreaks havoc on your emotional equilibrium, as well as your physical health. It narrows your ability to think clearly, function effectively, and enjoy life. Effective stress management, on the other hand, helps you break the hold stress has on your life, so you can be happier, healthier, and more productive. The ultimate goal is a balanced life, with time for work, relationships, relaxation, and funâ€”and the resilience to hold up under pressure and meet challenges head on. But stress management is not one-size-fits-all. The following stress management tips can help you do that. Identify the sources of stress in your life Stress management starts with identifying the sources of stress in your life. To identify your true sources of stress, look closely at your habits, attitude, and excuses: Do you blame your stress on other people or outside events, or view it as entirely normal and unexceptional? Until you accept responsibility for the role you play in creating or maintaining it, your stress level will remain outside your control. Start a stress journal A stress journal can help you identify the regular stressors in your life and the way you deal with them. Each time you feel stressed, keep track of it in your journal. As you keep a daily log, you will begin to see patterns and common themes. When handling such predictable stressors, you can either change the situation or change your reaction. Learn how to say "no. Whether in your personal or professional life, taking on more than you can handle is a surefire recipe for stress. Distinguish between the "shoulds" and the "musts" and, when possible, say "no" to taking on too much. Avoid people who stress you out. If someone consistently causes stress in your life, limit the amount of time you spend with that person, or end the relationship. Take control of your environment. If the evening news makes you anxious, turn off the TV. If traffic makes you tense, take a longer but less-traveled route. If going to the market is an unpleasant chore do your grocery shopping online. Pare down your to-do list. Analyze your schedule, responsibilities, and daily tasks. Often, this involves changing the way you communicate and operate in your daily life. Express your feelings instead of bottling them up. If something or someone is bothering you, be more assertive and communicate your concerns in an open and respectful way. Be willing to compromise. When you ask someone to change their behavior, be willing to do the same. Create a balanced schedule. All work and no play is a recipe for burnout. Try to find a balance between work and family life, social activities and solitary pursuits, daily responsibilities and downtime. You can adapt to stressful situations and regain your sense of control by changing your expectations and attitude. Try to view stressful situations from a more positive perspective. Rather than fuming about a traffic jam, look at it as an opportunity to pause and regroup, listen to your favorite radio station, or enjoy some alone time. Look at the big picture. Take perspective of the stressful situation. Ask yourself how important it will be in the long run. Will it matter in a month? Is it really worth getting upset over? If the answer is no, focus your time and energy elsewhere. Perfectionism is a major source of avoidable stress. Stop setting yourself up for failure by demanding perfection. When stress is getting you down, take a moment to reflect on all the things you appreciate in your life, including your own positive qualities and gifts. This simple strategy can help you keep things in perspective. In such cases, the best way to cope with stress is to accept things as they are. Many things in life are beyond our controlâ€”particularly the behavior of other people. Rather than stressing out over them, focus on the things you can control such as the way you choose to react to problems. Look for the upside. When facing major challenges, try to look at them as opportunities for personal growth. If your own poor choices contributed to a stressful situation, reflect on them and learn from your mistakes. Accept the fact that we live in an imperfect world and that people make mistakes. Let go of anger and resentments. Free yourself from negative energy by forgiving and moving on. Talk to a trusted friend or make an appointment with a therapist. Exercise releases endorphins that make you feel good, and it can also serve as a valuable distraction from your daily worries. Even very small activities can add up over the course of a day. The first step is to get yourself up and moving. Here are some easy ways to incorporate exercise into your daily schedule: Put on some music and dance around Take your dog for a walk Walk or cycle to the grocery store Use the stairs at home or work rather than an elevator Park your car in the farthest spot in the lot and walk the rest of the way Pair up with an exercise partner and encourage each other as you work out Play ping-pong or an activity-based video game with your kids The stress-busting magic of mindful rhythmic exercise While just about any form of physical activity can help burn away tension and stress, rhythmic activities are especially effective. Focus on coordinating your breathing with your movements, for example, or notice how the air or sunlight feels on your skin. Adding this mindfulness element will help you break out of the cycle of negative thoughts that often accompanies overwhelming stress. Connect to others There is nothing more calming than spending quality time with another human being who makes you feel safe and understood. So make it a point to connect regularlyâ€”and in personâ€”with family and friends. They simply need to be good listeners. And try not to let worries about looking weak or being a burden keep you from opening up. The people who care about you will be flattered by your trust. It will only strengthen your bond. Tips for building relationships Reach out to a colleague at work Help someone else by volunteering Have lunch or coffee with a friend Ask a loved one to check in with you regularly Accompany someone to the movies or a concert Call or email an old friend Go for a walk with a workout buddy Schedule a weekly dinner date Meet new people by taking a class or joining a club Confide in a clergy member, teacher, or sports coach Tip 5: Nurturing yourself is a necessity, not a luxury. Set aside leisure time. Include rest and relaxation in your daily schedule. This is your time to take a break from all responsibilities and recharge your batteries. Do something you enjoy every day. Make time for leisure activities that bring you joy, whether it be stargazing, playing the piano, or working on your bike. Keep your sense of humor. This includes the ability to laugh at yourself. The act of laughing helps your body fight stress in a number of ways. Ways to Relieve Stress Take up a relaxation practice. As you learn and practice these techniques, your stress levels will decrease and your mind and body will become calm and centered. Manage your time better Poor time management can cause a lot of stress. Stress and Your Health: Avoid scheduling things back-to-back or trying to fit too much into one day. All too often, we underestimate how long things will take. Make a list of tasks you have to do, and tackle them in order of importance. Do the high-priority items first. If you have something particularly unpleasant or stressful to do, get it over with early. The rest of your day will be more pleasant as a result. Break projects into small steps. If a large project seems overwhelming, make a step-by-step plan. Focus on one manageable step at a time, rather than taking on everything at once. If other people can take care of the task, why not let them? Let go of the desire to control or oversee every little step. Maintain balance with a healthy lifestyle In addition to regular exercise, there are other healthy lifestyle choices that can increase your resistance to stress.

7: Stress Management: Using Self-Help Techniques for Dealing with Stress

Pete Tosh of the Focus Group offers practical steps to reduce union vulnerability and increase employee engagement in your organization. Pete offers 10 specific points to illustrate how.

Vulnerabilities in desktops, servers, laptops and infrastructure are commonly involved in intrusions and incidents. For example, the Chthonic malware designed to steal banking details, exploits a known Microsoft Office vulnerability CVE Implementing a culturally inappropriate strategy for vulnerability remediation simply fails to be effective at reducing risk. With that in mind, here are six different strategies for reducing vulnerability risk. The Fire Brigade Strategy: Treat vulnerabilities as incidents and respond to them individually, remediating quickly under pressure. Have you ever met someone who really only works well with a tight deadline? Some organizations are the same way. If you work in a culture where routine processes are hard to execute and people only really respond to emergencies, then the best way to get something done is to tie it to a tight deadline. Fixing the highest risk vulnerabilities is better than doing nothing. Lots of residual vulnerability risk. By definition, this strategy is only going to hit the high profile vulnerabilities, leaving lots of opportunity for attackers behind. An incident response strategy is unlikely to affect the underlying causes of vulnerability proliferation within an organization. Potential for staff burnout. This is probably already a problem for this type of organization, but people eventually get burned out responding to emergencies. Identify the highest risk assets and fix them first, regardless of specific vulnerability conditions. Do you have system owners who largely correspond to assets or asset types? If your organization has processes and procedures built around assets, then this strategy may be very effective. Inefficient use of resources. Addressing individual assets ignores opportunities for systemic improvement. For example, 10 different system owners patching Java on 50 different systems without recognizing that there might be a better way to address Java holistically. Prioritize the vulnerabilities, fix the highest priorities first. Do you have effective workflow systems in place already? Can you assign a task and follow it to completion easily? If your organization operates like a well-oiled machine, then start feeding the machine vulnerabilities. Seriously effective at reducing vulnerability risk. Only as good as the priorities. Pick the wrong priorities, and you leave risk hanging around to be exploited. You might be really good at hitting each high risk vulnerability individually, but miss opportunities to make systemic changes to reduce vulnerability risk. Central Analysis, Distributed Work. Information security performs analysis of the vulnerability scanning results and provides very directed remediation instructions to the larger organization. Is Information Security a centralized group in a distributed organization? Systematic reduction of vulnerability risk. If the whole organization executes, then decisions can be made at the level of the whole organization. Done well, this can produce a very responsive information security practice. Lowest common denominator execution. A centralized analysis many be less tuned to individual execution. The whole organization can only move as fast as its slowest parts. Poor analysis, poor results. A misstep in analysis at the top affects all areas, leaving room for systemic problems in the cases of bad analysis. Board of Directors Strategy: Distributed Analysis and Work, Centralized Tracking. Identify metrics for tracking progress overall, then allow each group within the organization the freedom to reduce vulnerability risk as they see fit. Do the groups across your organization require autonomy in how they work? Do you work in a metrics-focused organization? If your organization likes independence and a results-oriented approach, then focus on the metrics and drive outcomes. Choosing metrics that matter to the business can drive for vulnerability risk reductions that matters, rather than With different groups executing differently, they can compete based on the metrics and drive improvement. Bad metrics, bad results. When groups compete, someone ends up at the bottom. Forget about vulnerabilities and focus on reducing the overall attack surface through aggressive implementation of least privilege and elimination of unnecessary services and systems. Measure the results with vulnerability risk metrics. Does your organization fail to decommission systems effectively? Do people install whatever they want on their systems? Dramatic vulnerability risk reduction. Since vulnerabilities exist in applications, eliminating the unneeded applications can dramatically eliminate vulnerabilities. Side-benefits of a well managed environment. Focusing on configurations and reducing attack surface will generally result in a more understood and managed environment, which can have benefits to the business around cost-reduction, operational efficiency, and stability. Limited duration of effectiveness. High priority risk gap. As you can see, there are a variety of strategies for reducing vulnerability risk. While employing the right tools can help, knowing how your organization operates is what will make the difference between an expensive product and an effective program. Key Takeaways and Improvement Opportunities , which is available for download [registration form required]. Image header courtesy of ShutterStock.

8: Best Practices for Reducing Your Attack Surface with Vulnerability Management

MANAGING YOUR FEELINGS: Reducing Your Emotional Vulnerability Body Channel. Improve your self-care Meeting your basic needs (hunger, thirst, rest, illness, discomfort/pain, hygiene, and exercise) can.

Treat Physical illness Do you have a physical illness that needs to be tended to? What things keep you from treating your physical illness? Take some time to think about this, and see what it would take for you to take care of your physical needs. Balance Eating How well do you eat? Do you eat too little? What kinds of food do you eat? Also, if you eat too little over a period of time, your body goes into starvation mode, and burns the food more slowly, trying to protect itself from starving. What foods make you feel good? What foods make you feel bad? How does eating a lot of sugar make you feel? The key here is to eat foods that are healthy and that make you feel good. Avoid Mood-Altering Drugs Alcohol and drugs can lower resistance to certain negative emotions. For example, I found that when I drank alcohol, I felt more depressed and sometimes more frightened. If you use drugs or alcohol, notice how they make you feel. If they are a problem in your life, can you get some help? Balance Sleep How much sleep makes you feel good? Some people do fine on hours, others need hours. Some people need to nap during the day. Learn to plan your schedule so that you get the sleep you need. Do you have trouble sleeping? Sleep is a big one for me. If I do not get enough sleep on a regular basis, I get irritable, short-tempered, my judgment is less good and I get upset much more easily. I have to work on it all the time. Get Exercise Regular exercise, besides being good for your heart, lungs, muscles and bones, stimulates chemicals in your brain called endorphins, which are natural antidepressants. We are talking about aerobic exercise, the kind that makes you out of breath. Do you get regular exercise? If not, is there something you can do for exercise, starting out with just a little? What kinds of things are you good at doing? Can you learn a new skill? What kinds of things give you a sense of mastery, of being good at something or meeting a challenge? Sometimes these things will be a little bit hard or challenging. Discussion f you are someone who has not yet incorporated some of these things into your life, perhaps you could make a plan for doing so, perhaps trying just one thing at a time. If you want to keep track of how you are doing at sleep, for instance, you might keep a little chart of what time you go to bed and how much sleep you get each night. Sometimes we are not really aware of how much sleep we get or what exactly we eat. You could use your diary card as a checkoff chart. The purpose of this section is to get you to take a look at these parts of your life. Notice what you do and how you feel. Once you are aware of which areas are working well and which you would like to improve, you can choose something to work on.

9: Best Practices For Minimizing Business Travel Risk

One of the best ways to reduce your vulnerability to these distressing emotions you've identified is to optimize your physical health. You may not realize it, but exercising, getting enough sleep and eating healthy foods are as important to your mental and emotional health as they are to your physical health.

It is a necessity. But building and maintaining a fully functional SOC is a daunting proposition. Hiring, training, and retaining the necessary talent to staff a SOC is flatly impractical for many businesses. Included in this webinar are: Quick to engage on risk and response, Mr. Suby habitually examines emerging cybersecurity technologies before they reach mainstream. Suby is also intimately involved in researching how traditional cybersecurity solutions and platforms are addressing the diverse challenges and pressures encountered by IT and security practitioners. Oct 26 59 mins Sonu Shankar - Sr. Product Marketing Manager - Arctic Wolf Networks Organizations of all sizes are increasingly adopting cloud services to transform business processes. Unfortunately, the cloud also brings serious security concerns. SaaS applications add new attack surfaces beyond the traditional network perimeter, with employees accessing business data on various devices and from multiple locations. In this borderless ecosystem, adopting a fragmented approach to securing on-premises infrastructure, endpoints, and cloud resources, like SaaS apps, has proven to be dangerously ineffective. As early as , the average business experienced around 23 cloud-based security incidents each month. That number is rapidly rising, indicative of the need for a new, centralized approach to security. While larger enterprises can achieve comprehensive coverage across cloud and on-premises resources with a 24x7 security operations center SOC , smaller businesses may be leaving their critical infrastructure exposed. Without the resources to build an in-house SOC, or the ability to hire a large internal team of security experts to operate the SOC, what can you do to secure your data and network infrastructure? In this Arctic Wolf webinar, we dive into: In this webinar clip, hear his insights into how to respond to a data breach and how you determine the complexity or extent of that breach. To watch the full webinar, click here: Oct 18 40 mins Todd Thiemann, Director Product Marketing - Arctic Wolf Networks Financial institutions face a daunting combination of cybersecurity threats and compliance requirements. IT teams at regional banks and credit unions have a relatively small staff but facing similar security and compliance burden to what larger, well-resourced financial institutions carry. How can small and mid-sized financial institutions counter sophisticated cyberthreats, provide monitoring and incident response needed for compliance, and do so with tight budgets that do not allow for staffing an elaborate security operations center? Attend this webinar and learn about: Oct 12 3 mins Sonu Shankar - Sr. Threats that were relevant in the on-premises world may not be relevant anymore. We have to start thinking about new threats that danger our cloud. IT leaders are now responsible for connecting doctors, nurses, patients, and medical devices, or enabling financial advisors on the road, to deliver services to their clients. From enabling services via remote mobile devices, to managing IP-connected cameras on-premises at the same time, running this new converged IT ecosystem, that includes Operational Technology OT , can be a daunting task. Especially when your attack surface has now dramatically expanded. With the rise in data breaches in these industries, and the responsibility to manage this connected ecosystem, how do you protect your business from attacks targeting connected devices? Join us to discover: This is especially true with mid-market companies, where shrinking IT security budgets and shortage of skilled cyber security resources have forced them to reconsider investing in a SIEM, and seriously look at managed security services options. In this webinar, hear from security experts on: Business Drivers for Vulnerability Management Recorded: Director of Product Marketing, Arctic Wolf Networks, explores business drives for vulnerability management and how to reduce your attack surfaces. Sep 25 40 mins Narayan Makaram, Senior Director of Product Marketing, Arctic Wolf Networks With the major cyber-attacks headlining the news, many of these cyber threats fall into five different attack vectors. So, how do you protect you and your business from these debilitating attacks? In our upcoming webinar, we arm you with the essential components needed to defend your business against the top five attack vectors we see in a Cyber Security Operations Center SOC. After attending you will: These various strains of Ransomware can bypass your perimeter controls and infect your critical systems, bringing your business to a grinding halt. However, focusing on prevention technologies, with point security products, may not be sufficient enough to fight these key security concerns. So, what are your options? About our key speaker: Dinah holds an M. Math in cryptography from the University of Waterloo. To Outsource, or Not To Outsource: In addition, many businesses are increasingly relying on network and cloud service providers, taking key security functions out of their hands. How can enterprise security teams work with third-party contractors and service providers to improve overall security? Sep 13 3 mins Todd Thiemann, Director Product Marketing - Arctic Wolf Networks In this webinar clip, we dive into the impact a data breach can have for financial institutions. With smaller IT teams, regional banks and credit unions face similar security and compliance burdens to what larger, well-resourced financial institutions carry. So, what can you do if breached? To hear more from our security experts and how to solve the financial services security talent shortage with managed detection, click here: Sep 10 3 mins Todd Thiemann, Director Product Marketing - Arctic Wolf Networks In this insightful webinar clip, we provide brief insights into how you can manage cyberthreats. Regional banks and credit unions often face the same security and compliance burdens to larger, well-resourced financial institutions with much smaller staffs. So, what should your security plan for managing cyberthreats look like?

MINIMIZING YOUR VULNERABILITY pdf

The travelers guide to Middle Eastern and North African customs and manners Otitis Media in Infants and Children 4/E (Otitis Media in Infants Children (BlueStone/Klein)) The Atlantic Ocean (True Books) Dangling on a string Apple ipad 2 instruction manual Hiring and employment practices and the law Doll-house Accessories, How to Design and Make Them. The message of the Virgin Marys global presence-understanding the why of the apparitions Electricity sector law, 5756-1996. Alabama state university undergraduate application Just Across the Fields The numbers that count Just ing and writing elementary Sunil gangopadhyay story books People of the north, people of the west, people of the east, people of the south, dress What was it like before television? Two kinds of patriots The elements of game design The Secret of Sinharat and People of the Talisman The whole Bible is a missionary book Slk r170 workshop manual Hunger of memory full From the Other Shore The Russian People and Socialism Ancient and Medieval Modelling (Modelling Masterclass) I dread Christmas Spectrum Language Arts, Grade 6 (Spectrum (McGraw-Hill)) Tomato plant girl Outlines Highlights for Politics in America by Dye, ISBN Fox Terriers (Complete Pet Owners Manuals) Lessons from the genomes: microbial ecology and genomics Andrew S. Whiteley . [et al] What is the fourth-grade child like? 2003 chevy avalanche service manual Ch. 8. Addressing corruption and organized crime in the context of re-establishing the rule of law Sebast Suite seduction jm jeffries Ken Tyrell The Man and His Cars And Gas Chromatography-Olfactometry100 Business funding proposal sample Life sciences before the twentieth century Traffic officer application form 2017 An after-dinners sleep