HITACHI
Inspire the Next

Vulnerability assessments:

GAUGING THE HEALTH OF YOUR SECURITY PROGRAM

Hitachi Systems Security Inc.

TABLE OF CONTENTS

INTRODUCTION

Just like a physical or stress test, vulnerability assessments are geared to uncover weaknesses in your company's security condition before they become problems.

As your company's dependence on technology increases and you introduce additional electronic systems and software to support your operations, the rate of discovering and exploiting software vulnerabilities will continue to rise. Vulnerabilities put organizations and their customers' data at risk. Getting a clear understanding of your organization's level of protection is critical when mitigating cyberattacks. Sixty percent of small businesses close within six months of a cyber attack.

Protect your organization and your customers.

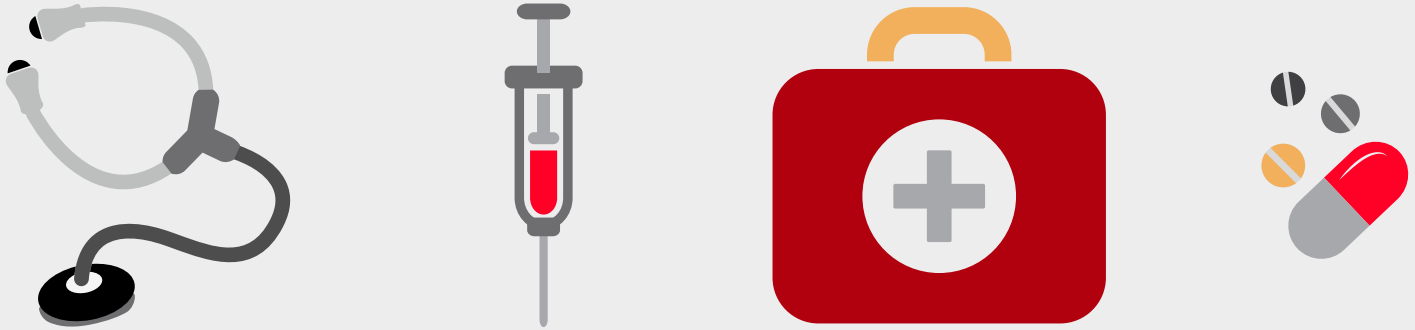
This e-book provides facts and insights about how you can develop a strong and healthy security program for your organization.

WHAT IS A VULNERABILITY ASSESSMENT?

A vulnerability assessment is a process that identifies and quantifies the security weaknesses within your software, hardware and network.

With a vulnerability assessment, you can:

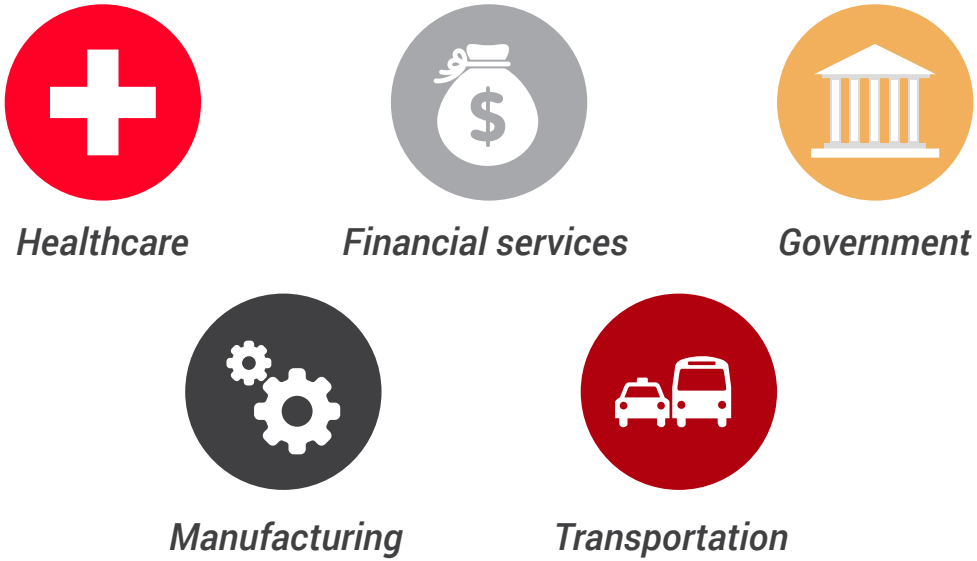
- Evaluate your IT security posture;
- Uncover weaknesses; and
- Provide the appropriate mitigation procedures required to either eliminate those weaknesses or manage them within your risk management strategy.



DO WE NEED A VULNERABILITY ASSESSMENT?

While reactive teams spend their time covering security weaknesses with cyber Band-Aids, proactive teams use vulnerability assessments to assess their security posture so they can determine the severity of their vulnerabilities and create a plan, with the help of an experienced partner, to understand, measure, and strategically reduce their exposure to overall IT security risk.

Industries that are most likely to be targeted by cybercriminals include*:



86%
of businesses would remove a supplier due to a breach.**

*Verizon 2016 Data Breach Investigations Report ** Verizon 2015 Data Breach Investigation Report

HOW DOES A VULNERABILITY ASSESSMENT HELP MY COMPANY?

The best way to take this first step in improving your IT security is to find a partner who can guide you through the process and the steps that – *ideally* – will follow. Regular vulnerability assessments can help your company:

- Identify known security issues before attackers target them.
- Create an inventory of all the devices on the network, including purpose and system information. This also includeds vulnerabilities associated with specific devices.
- Create an inventory of all devices in the enterprise to help with planning of upgrades and future assessments.
- Define the level of risk that exists on the network.
- Establish a business risk/benefit curve and optimize security investments.

To fully capture these benefits, you must view the vulnerability assessment as your initial measurement in an ongoing process period geared to improve organizational security posture.

4 KEY VULNERABILITY ASSESSMENT STEPS TO KEEP YOUR COMPANY HEALTHY

1. Catalogue assets and resources in a system.
2. Assign quantifiable value and importance to assets and data.
3. Identify security vulnerabilities or potential threats to assets and develop a strategy to deal with the most serious threats first.
4. Mitigate or eliminate the most serious vulnerabilities for the most critical assets.

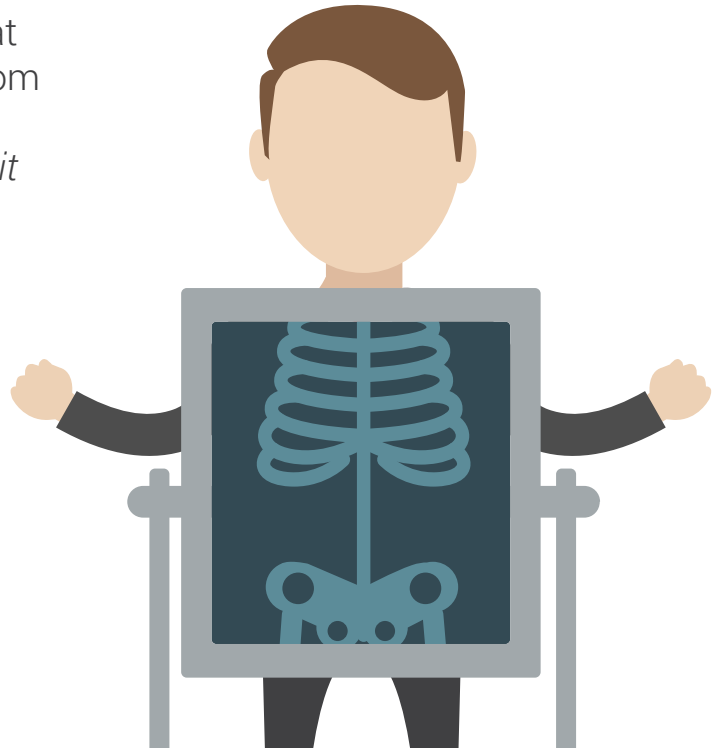
Getting a clear understanding of your organization's level of protection is critical in defending against cyberattacks.

CAN'T I DO THE VULNERABILITY ASSESSMENT MYSELF?

Organizations have tried this, but similar to assessing your own level of health, it has proven to be less effective and often neglects serious risks.

Further, there are several automated tools out there that allow you to perform assessments yourself, but at the end of the day, vulnerability assessments deliver reams of data that require analysis. Some of it might indicate the need for a simple patch, and some of it might indicate a serious problem that requires server hardening, network reconfiguration or other extensive responses. Having an expert on hand to help you identify the difference is essential.

Before you engage with a vendor, make sure you know what you'll get. You'll want someone who will sit down across from you after the assessment, explain the resulting report and recommend a roadmap to remedy security gaps – *then do it all again when it's time for your next vulnerability assessment.*



60%

of organizations breached in minutes or less.*

** Verizon 2016 Data Breach Investigation Report*

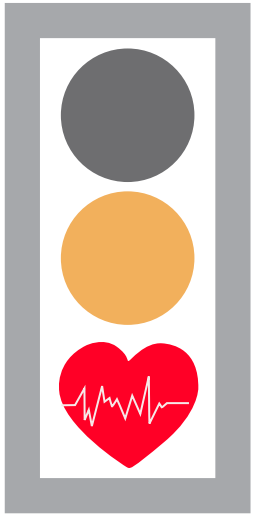
3 PHASES OF A VULNERABILITY ASSESSMENT

Get ready...

Before you conduct your assessments, establish the boundaries of your two main objectives: planning and performance. In the planning stage, you'll want to gather relevant information, define the scope of activities, and define the roles and responsibilities for informing internal teams about changes to the management process. In the performing stage, interview system administrators and review the policies and procedures related to the systems you'll be scanning.

Get set...

Once you've identified potential security issues, review the results with stakeholders, and tie them to your processes. This is an important step to ensuring issues are established and vulnerabilities resolved. This is also the time for storing and reviewing data for companywide risk analysis and trending.



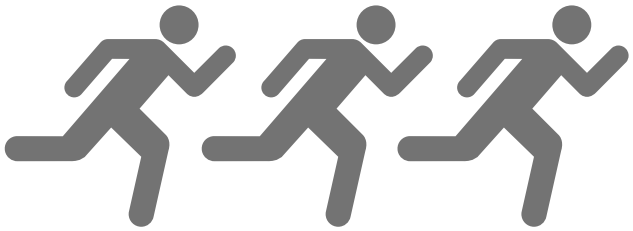
Go!

A vulnerability assessment is only as useful as the plan that follows it and execution of that plan. Figure out which vulnerabilities need fixing and address the ones that represent the highest risk to the company in priority order.

HOW OFTEN SHOULD WE CONDUCT VULNERABILITY ASSESSMENTS?

A vulnerability assessment provides an accurate point-in-time representation of your security posture, but one point in time is not enough to secure your IT assets and resources. Conduct vulnerability assessments semiannually, annually, or when significant system changes occur for best results.

Want to outrun attackers in a high-risk industry?



Work continuous vulnerability assessments into your routine.

Want to secure your small business in a low-risk industry or geography?

Conduct vulnerability assessments semiannually (at the very least).

WHAT DO WE DO AFTER A VULNERABILITY ASSESSMENT?

Your vulnerability assessment reports – *like the vital signs your doctor takes during your medical checkups* – need the interpretation and insight of a trained professional. It's crucial to work with an expert to determine which vulnerabilities require updating programs and which demand more in depth remediation. In many respects, it's like getting an MRI scan of all your systems. Are they healthy or not? And which treatments will be most effective in bringing your customer databases, servers and other IT assets back to good health?

Answering those questions will lead you into the next steps in the process – ***penetration testing, vulnerability management*** and ***overall risk management*** prior to setting goals for your next vulnerability assessment.

About Hitachi Systems Security

Since 1999, Hitachi Systems Security has helped companies identify and repair their vulnerabilities to secure their most sensitive IT assets. Ready to talk to an IT security specialist about your vulnerability management strategy?

Hitachi Systems Company is a Global IT Security Service Provider who builds and delivers customized services for monitoring and protecting the most critical and sensitive IT assets in our clients' infrastructures 24/7. With a relentless focus on risk management, and continuous improvement of our technology and incident response processes, our clients count on us to provide the right solutions for their businesses -quickly, effectively and with expertise beyond the industry standards. Our mission is to deploy information security solutions that protect our customer's brand, and allow them to harness the full potential of connecting people and businesses together to build trusting relationships that can be catalyst of worry-free collaboration and limitless potential.

Being ISO 9001:2008 certified for its Managed Security Service delivery from its World Headquarters, Hitachi Systems Security is also an accredited member of FIRST (Forum of Incident Response and Security Teams) and a Certified QSA (Qualified Security Assessor) for Canada, the United States, Latin America and the Caribbean from the Payment Card Industry Security Standards Council (PCI SSC).

www.hitachi-systems-security.com | info@hitachi-systems-security.com
+1 (450) 430-8166 | +1 (866) 430-8166 (toll free)

Contact us.

Choose a vulnerability assessment partner who can help you understand and make a roadmap for success. It helps to have one that can strategically conduct pen tests after your company's vulnerabilities are surfaced.

Hitachi Systems Security Inc.