PACIFIC NORTHWEST NATIONAL LABORATORY

The opinions expressed by the presenters are the opinions of the presenters and are not the opinions of Battelle Memorial Institute or the Pacific Northwest National Laboratory. Battelle's role in supporting this seminar is a part of its service to the public and does not: (1) constitute an endorsement of the presenters, the presenters' opinions, or the organizations represented by the presenters; or (2) represent a recommendation of any services, strategies or products discussed during this presentation. This seminar is presented for educational purposes only.

Pacific North



Networks and servers and hackers... oh my! The risks of using and relying on technology

Monday, November 23, 2009

nGenuity helps businesses safeguard their valuable information from the risks posed by today's high-tech environment.

Utilizing analytical processes and technology solutions, our consultants assess risk and recommend measures that ensure your information is secure, and that critical networks and computer systems are running smoothly.

Staffed with nationally accredited security consultants, nGenuity possesses over 20 years of combined IT security experience.

Ensure the protection of your most valuable data.



Technology in our day

- 7:30 AM Check mobile phone for daily schedule
- 7:55 AM Badge into the office
- 8:00 AM Check Email
- 8:05 AM Blog / tweet / facebook, check stocks
- 9:00 AM Order from Website
- 9:45 AM Print agenda for morning meeting
- 11:00 AM Receive reports from Accounting
- 1:00 PM Call conference bridge for finance meeting

Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

The typical business relies on technology every day in a number of ways. Ways that you might never expected to be so important to your business.



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

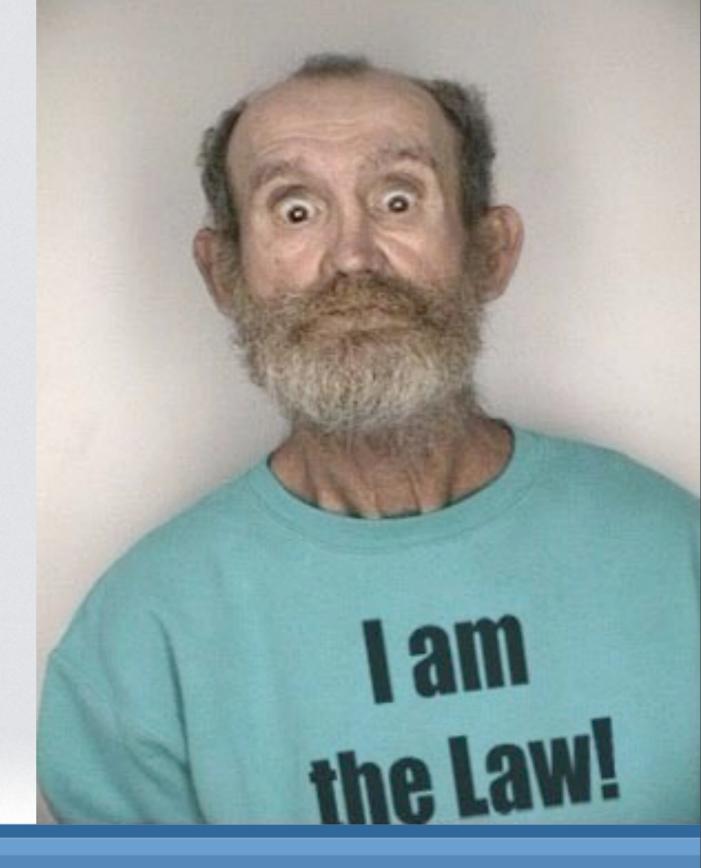


Monday, November 23, 2009

The risks we will focus on are People and Technology.



People



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

People are an often ignored risk. We ignore the fact that we are lazy and forgetful. Simply being aware of this fact allows us to implement compensating technical controls. People are also motivated by factors other than logic, money, emotion, etc.

nGenuity

Social engineering



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

More information on social engineering can be found at social-engineer.org



Mistakes & accidents



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!



Malicious insiders



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

For most businesses in my experience get the most attacks from outside of the organization. The most damaging ones I see come from inside attackers. This might be a malicious or disgruntled employee. Doing proper background checks and auditing employee activities for privileged employees will help mitigate this.



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!



Web apps & sites



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

When it comes to technology threats, web applications are often times the only exposure an organization has to the Internet and often the most mis-understood risk. Web applications often allow outside access into our networks and are connected to databases, by passing firewalls and other protection controls we may have in place.



64 is a lot of percent.

"64% of websites currently have at least one serious vulnerability."

- Whitehat Security

Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!



Exploitation demonstration



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

Using the SET (Social Engineers Toolkit) available from social-engineer.org I demonstrated just how easy attackers have it when attacking end users. Going back to the end user as the weakest link, when users simply click "ok" or "run" and ignore browser warnings, it's rather easy to take over systems.



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!



So should we just give up and close up shop?



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

Attackers have the upper hand in most cases. As defenders we have to find and compensate for every vulnerability and they have to just find one to be able to potentially exploit us. There are no guarantees in security only reduction and management of risk. Following a well defined process will assist with identification and mitigation of risk.



Assess

Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

Assess:

Assessments are the starting point of any process. They help identify areas of vulnerability. There are many types of assessments that specific areas of the organization.

A few important ones to focus on are: Policy Gap Analysis Web application Assessment Network Penetration Test



Hostgator



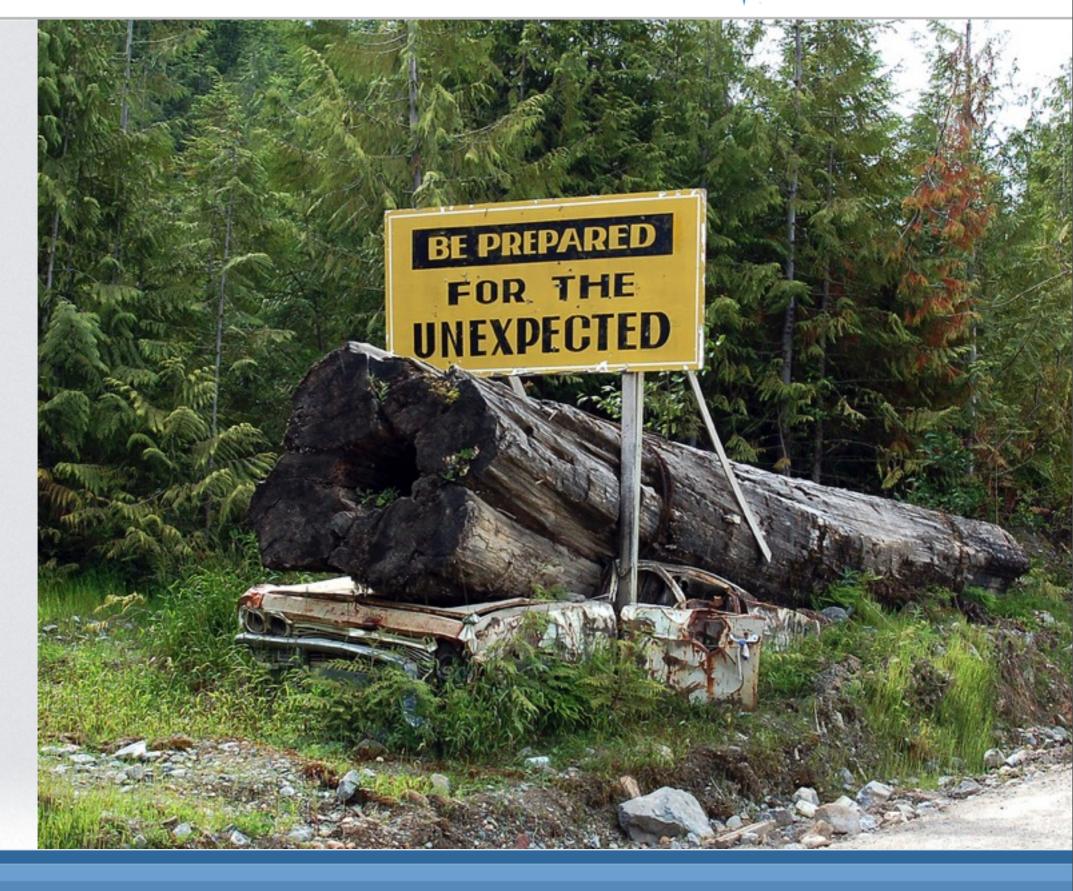
Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

Hostgator.com hosts 2.2 million domains. nGenuity provided web application and code assessment services for an in-house developed application.



Plan



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

Plan:

Don't bother purchasing technology unless you know where your starting (assessment) and know where you want to end up (plan).

nGenuity

Protect



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

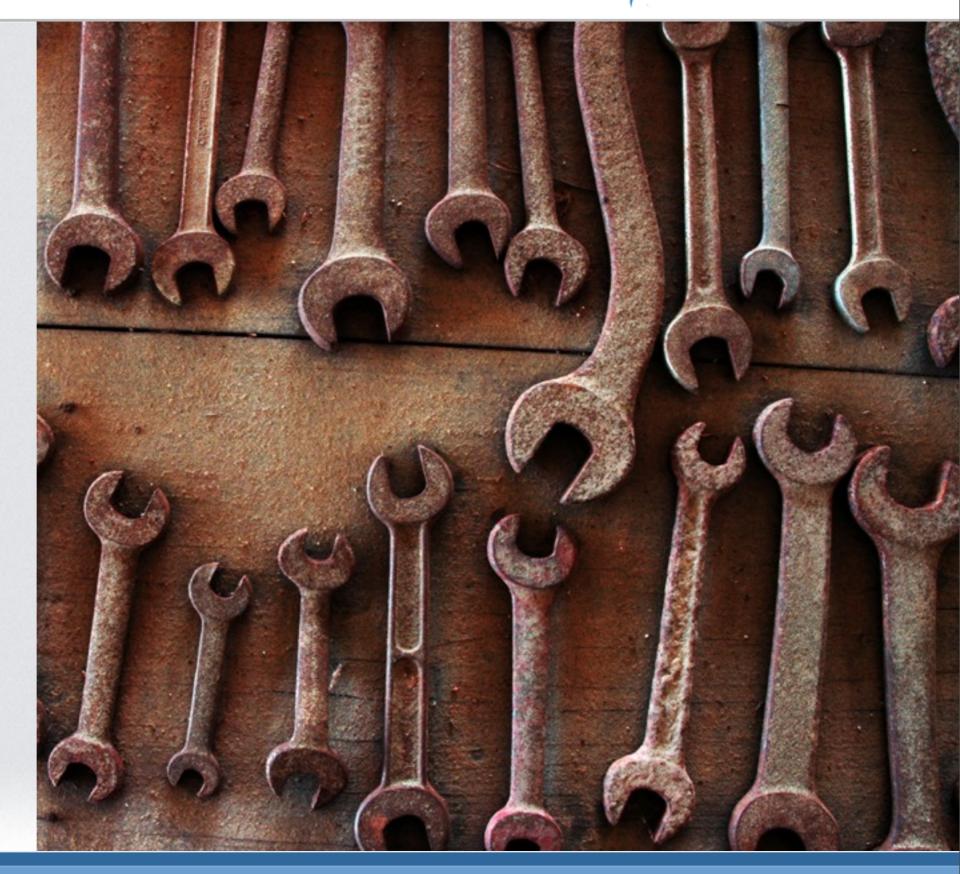
Monday, November 23, 2009

Protect:

Implement the technical controls and training that gets to mitigating and reducing the risk that is outlined in your plan.



Maintain



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!

Monday, November 23, 2009

Security is not set and forget. You must constantly take a pulse on the security of the organization and adjust to make sure you are making effective use of your security controls.



Adam Baldwin // TREN // Nov. 17, 2009 // Networks and servers and hackers... oh, my!



Questions?

Adam Baldwin // lockonit.com // 509.396.2075

Monday, November 23, 2009

Template design by &yet (andyet.net)