Implementing Secure Software Development — A Method that’s Guaranteed to Work!
The Ohio Information Security Conference 2015

By: Ann Gallaher, COO, Technology First

Welcome! The Ohio Information Security Conference is a technical conference targeted to business owners, managers, and security professionals who have a vested interest in protecting their company’s information and communication systems. The conference is hosted each year by Technology First at Sinclair Community College and will offer four breakout tracks and three keynote presentations.

The Breakfast Keynote speaker this year will be presented by Waylon Krush, CISSP, CISA, CAP, and the CEO, of Lunarline. He will discuss how attacks against the logical world of computers and networks undermines our physical safety.

The luncheon keynote will be John S. Bommer, Jr. who was the former Director, Cyberspace Professional Continuing Education, Center for Cyberspace Research Air Force Institute of Technology. In Mr. Bommer’s presentation, Changing Security Laws — Federal and International Legislation, he will discuss the intrinsic value of changing security laws and how governing communities could restructure our Internet Global Economic Commerce lanes and systematically disable the criminal hacker groups.

SSA Kevin P. Rojek, Squad 13, Cyber Cincinnati Field Office, of the Federal Bureau of Investigation will present the reception keynote. Agent Rojek will explain the need to understand the threat and remain one-step ahead of the criminals who seek to steal our money, pilfer our intellectual property, and threaten our livelihood.

This year is the 12th annual Ohio Information Security Conference. Again, it has been organized by local information security professionals to focus on emerging trends and share on industry insights. They are certain this event will provide a networking environment to meet and learn from professionals around the state who share similar challenges and requirements. We would like to recognize those committee members contributing to the success of the conference.

Steve Walker ................. Premier Health
Deral Heiland ................. Rapid7
Leo Cronin ....................... Cincinnati Bell
Dave Salisbury .............. University of Dayton
Phil Woods
John Hermes ................. OIS Forum
Tim Shaw ......................... ATIC
<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Location</th>
<th>Speaker/Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:45–8:30</td>
<td>Registration and Breakfast</td>
<td>Charity Auditorium</td>
<td>Waylon Krush, CISSP, CISA, Co-Founder and CEO, Lunarline, Inc</td>
</tr>
<tr>
<td>8:30–9:30</td>
<td><strong>BREAKFAST KEYNOTE:</strong></td>
<td>Charity Auditorium</td>
<td>A Logical Leap — How Modern Cyber Attacks Threaten our Physical Safety</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Waylon Krush, CISSP, CISA, Co-Founder and CEO, Lunarline, Inc</td>
</tr>
<tr>
<td>9:45–10:45</td>
<td>A Risk-based Approach to Identity Management</td>
<td>Room # 131 120 127 116</td>
<td>Kampmann, Gartner</td>
</tr>
<tr>
<td>9:45–10:45</td>
<td>Compliance vs. Security — How to Build a Secure Compliance Program</td>
<td>Room # 131 120 127 116</td>
<td>Foresman, Rook Security</td>
</tr>
<tr>
<td>9:45–10:45</td>
<td>A Gentle Introduction into Quantum Key Distribution Technology</td>
<td>Room # 131 120 127 116</td>
<td>Grimalia, AFIT</td>
</tr>
<tr>
<td>9:45–10:45</td>
<td>A Detailed Break Down of a Data Breach</td>
<td>Room # 131 120 127 116</td>
<td>Havelt, McGladrey</td>
</tr>
<tr>
<td>10:45–11:10</td>
<td>Networking and Exhibition Time</td>
<td>Charity Auditorium</td>
<td>Bennett, Taft</td>
</tr>
<tr>
<td>10:45–11:10</td>
<td>Ascending Everest: Managing Third-party Risk in the Modern Enterprise</td>
<td>Charity Auditorium</td>
<td>Eck, Forsythe</td>
</tr>
<tr>
<td>10:45–11:10</td>
<td>Simulating Cyber Operations: “Do you want to play a game?”</td>
<td>Charity Auditorium</td>
<td>Fite, BT</td>
</tr>
<tr>
<td>10:45–11:10</td>
<td>The Trust Factor: How Social Engineering is Hacking the Mind</td>
<td>Charity Auditorium</td>
<td>Pelletier, Pondurance</td>
</tr>
<tr>
<td>12:00–1:30</td>
<td><strong>LUNCH KEYNOTE:</strong></td>
<td>Charity Auditorium</td>
<td>Changing Security Laws — Federal and International Legislation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>John S. Bommer, Jr., Former Director, Cyberspace Professional Continuing Education, Center For Cyberspace Research Air Force Institute Of Technology</td>
</tr>
<tr>
<td>Room #</td>
<td>131 120 127 116</td>
<td></td>
<td>Presentation from 12:30 to 1:15 pm</td>
</tr>
<tr>
<td>1:45–2:45</td>
<td>Insurance Coverage for Privacy and Data Breaches — Hot Topics and Critical Issues</td>
<td>Room # 131 120 127 116</td>
<td>Wagner, Taft</td>
</tr>
<tr>
<td>1:45–2:45</td>
<td>Does Anyone Remember Enterprise Security Architecture?</td>
<td>Room # 131 120 127 116</td>
<td>Brockway, Black Box</td>
</tr>
<tr>
<td>1:45–2:45</td>
<td>Cyber Tradecraft or Espionage?</td>
<td>Room # 131 120 127 116</td>
<td>Booz Allen Hamilton</td>
</tr>
<tr>
<td>3:00–4:00</td>
<td>Building Better Business Cases with Quantitative Risk Analysis</td>
<td>Room # 131 120 127 116</td>
<td>Garcia, HealthGuard</td>
</tr>
<tr>
<td>3:00–4:00</td>
<td>The Physical Security Evolution: Bridging the Divide between Facilities Management and IT</td>
<td>Room # 131 120 127 116</td>
<td>Blair, Savvux</td>
</tr>
<tr>
<td>3:00–4:00</td>
<td>Why Not Trust Your Hardware?</td>
<td>Room # 131 120 127 116</td>
<td>O’Hair, ATIC</td>
</tr>
<tr>
<td>4:10–5:00</td>
<td><strong>FINAL KEYNOTE:</strong></td>
<td>Charity Auditorium</td>
<td>Current Cyber Threats: An Ever Changing Landscape</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Corey Collins, Acting Supervisor, Cyber &amp; Technical Services Squad, Federal Bureau of Investigation</td>
</tr>
</tbody>
</table>
KEYNOTE SPEAKERS

LUNCH KEYNOTE:

Changing Security Laws — Federal and International Legislation

John S. Bommer, Jr., Former Director, Center for Cyberspace Research, AFIT


He has twenty years of leadership and technical experience in government operations of cyberspace, telecommunications, intelligence, and military agencies, including specialized skills in tactical, operational and strategic cyberspace and information assurance planning, systems analysis, operational assessments and alternative analysis, legislative affairs and program management.

As a cyber-security educator, he developed curriculum and educated cyberspace professionals, verified computer-based simulations, and implemented executive-level strategy. As an Air Force squadron commander, John oversaw the delivery of IT services, including requirements and feasibility analyses, IT procurements, software implementation, network management, communications systems, maintenance of Air Force corporate systems, infrastructure support, and network and data security.

Most recently John served as the Director, Cyberspace Professional Continuing Education Center for Cyberspace Research Air Force Institute of Technology.

PRESENTATIONS 9:45–10:45 am

Room 131
9:45–10:45 am

A Risk-based Approach to Identity Management

Kampmann, Gartner

Managing identity information and access privileges on an on-going basis is an area where demonstrating benefits is often challenging. Adopting a risk-based approach changes the dialog from an administrative activity to a threat management approach. This improves the viability and understanding of identity management and demonstrates its importance in the overall security portfolio. This session will introduce a risk model that can be employed to improve communications with business and security management.

BIO: Mr. Kampmann has over 30 years of experience in identity and security management. In his career with Gartner he has worked as a consultant and as a technology analyst. He specializes in financial services, higher education and health services. His published research includes identity management, infrastructure, collaboration, risk and compliance. He has acted in leadership positions in the development of industry standards for directory services and identity services.

Room 127
9:45–10:45 am

A Gentle Introduction into Quantum Key Distribution Technology

Dr. Michael R. Grimaila, AFIT

Quantum Key Distribution (QKD) is a revolutionary security technology that exploits the laws of quantum mechanics to achieve information-theoretic secure key exchange. In this presentation, I provide background and the basic principles of QKD and discuss vulnerabilities arising from the non-idealities present in real world QKD system implementations.

BIO: Dr. Michael R. Grimaila is a Professor of Systems Engineering and member of the Center for Cyberspace Research at the Air Force Institute of Technology, Wright-Patterson AFB. He has published over 100 technical papers in the areas of computer security, information security, and mission assurance.

Room 120
9:45–10:45 am

Compliance vs. Security — How to Build a Secure Compliance Program

Jeff Foresman, Rook Security

The large number of data breaches in 2014 clearly demonstrates that organizations that achieve regulatory compliance are not necessarily secure. We will look at the challenges companies face in achieving compliance standards such as PCI DSS and HIPAA as well as the mistakes made in maintaining a secure IT environment.

BIO: Jeff Foresman, Compliance Lead at Rook Security, specializes in PCI, HIPAA, GLBA, ISO 27000, and NIST 800-53 consulting and advisory services. He also serves as the President of the Central Indiana Information Security Systems Association (ISSA) chapter and is a frequent speaker at regional and national information security events. Jeff assists clients with developing and implementing information security programs including policies, procedures, awareness training, data discovery, and data classification programs to protect client’s data. Prior to joining Rook Security, Jeff worked for the PCI Security Council, Verizon Business, Pondurance, and Sarcom, where he collectively gained 20 years of IT experience and 14 years of information security experience.

Room 116
9:45–10:45 am

A Detailed Break Down of a Data Breach

Rob Havelt, McGladrey

Hackers are constantly using a myriad of evolving and changing techniques to break into organizations and steal data of value to them. In this presentation we will discuss at a step by step level how a recent major data breach at a retailer was accomplished. How the attacker used technical, social engineering, custom malware, and common tools to break into the organization and infiltrate approximately $80 million dollars worth of information in a matter of a couple of weeks.

BIO: Rob Havelt is a Director with the Security and Privacy Services group at McGladrey where he serves as the firm’s national leader for Security Testing. He specializes in penetration testing, wireless technologies, application security, offensive security, and threat modeling. Rob has over 20 years of professional experience in a wide array of information security disciplines.
Corey Collins, Acting Supervisor, Cyber & Technical Services Squad, Federal Bureau of Investigation

Special Agent Collins holds a bachelor’s degree in computer engineering. He currently investigates network intrusions, online fraud, theft of trade secrets, and innocent images and crimes against children. Special Agent Collins works actively to assist local and other federal law enforcement agencies to investigate computer-related criminal activity.

Jackie Bennett, Taft

Increasingly, in-house counsel find themselves being confronted with the unlawful accessing and pilfering of their company’s confidential electronic data by hackers. Thefts of a company’s private data—which may include highly confidential personal and financial information of employees, clients, customers, patients and vendors—are not merely embarrassing, but also may result in serious financial and legal liability. This presentation will focus on the key steps that should be taken by companies to respond to data breaches and what to expect in dealing with regulatory and law enforcement agencies.

BIO: Jackie Bennett is a commercial and white-collar criminal litigator with extensive experience in representing individuals and companies before agencies in state and federal courts. Prior to entering private practice, Jackie was a long time federal prosecutor with the Justice Department in Washington, D.C., where he was involved in numerous high profile investigations and trials of political officials.

Ron Pelletier, Pondurance

The human element that represents the greatest security threat to organizations today. Are people too trusting, too afraid, or too reticent to question someone they find suspicious? This presentation will perform a social engineering case study and examine what went wrong, how companies can educate their employees better and next steps to securing your infrastructure from emerging threats.

BIO: Ron Pelletier is certified in multiple disciplines relating to information and asset protection including Certified Information Systems Security Professional (CISSP), Certified Information Systems Security Manager (CISM), Certified Business Continuity Professional (CBCP), Certified Information Systems Auditor (CISA), Certified Computer Forensics Examiner (CCFE), and Certified Ethical Hacker (CEH).

Thomas Eck, Forsythe

Many recent information security breaches can be traced back to the compromised organization’s third-party risk management practices. New strategies will be presented that can help your organization move beyond technology-based solutions, questionnaires, contract language and trust to tackle the monumental task of managing third-party risk within the enterprise.

BIO: Thomas Eck, Practice Manager, IT Risk Management Programs, leads a team of consultants focused on helping Forsythe’s clients develop and refine their IT risk management strategies. He graduated as a Fuqua Scholar from Duke University’s Global Executive MBA program and is also the author of several books and magazine articles.

Bryan K. Fite, BT

It’s not polite to hack your neighbor but how else can a nation-state train and assess cyber warriors? Simulations and games are an effective approach. However, there are many cyber security games, competitions and training platforms. They vary widely in effectiveness, assessment capabilities and flexibility. In addition, most are closed and proprietary in nature. What is needed is a publicly adopted cyber operations simulation standard to support training, assessment and tool & technique development across platforms. I will share an innovative way to describe Cyber Operations Simulation elements by abstracting the primitives and describing their interaction via a Scenarios Definition Language. I will describe the methodology & approach, fundamental object types and teach attendees how to run their own simulations the Packetwars way!

BIO: Bryan K. Fite: A committed security practitioner and entrepreneur, Bryan is currently a Senior Security Consultant for BT. Having spent over 25 years in mission-critical environments, Bryan is uniquely qualified to advise organizations on what works and what doesn’t. Bryan has worked with organizations in every major vertical throughout the world and has established himself as a trusted advisor. “The challenges facing organizations today require a business reasonable approach to managing risk, trust and limited resources while protecting what matters.”
Room 131
1:45–2:45 pm

Insurance Coverage for Privacy and Data Breaches — Hot Topics and Critical Issues

Bill Wagner, Taft

This presentation will focus on hot topics and critical issues regarding insurance coverage for privacy and data breaches. It will begin with a basic introduction into the costs and consequences resulting from privacy and data breaches and a general discussion of the parties and types of claims being asserted. It will examine the types of claims policy holders have asserted under CGL policies, including under Coverage A for bodily injury and property damage and Coverage B for personal and advertising injury, and defenses asserted by insurers, and how the claims are being resolved in the courts. It will examine the new Insurance Services Office, Inc. privacy and data liability exclusions (a brief overview). It will then discuss the new cyber risk policies and issues related to what they say they cover and the types of defenses asserted by insurers to deny coverage. Finally, it will discuss the critical issues when negotiating to purchase insurance coverage to cover the types of risks and claims previously discussed.

BIO: Bill Wagner is a seasoned trial attorney with Taft who has helped clients maximize their insurance coverage as part of a comprehensive risk management and cost savings strategy. He has extensive experience litigating insurance coverage disputes for both policy holders and defending insurers pursuing equitable contribution claims against other insurance companies. He also has extensive experience working with business owners, officers, senior management, and general counsel analyzing risks, reviewing existing insurance policies, negotiating key terms and conditions, and litigating insurance coverage claims. Bill has successfully litigated insurance coverage disputes involving commercial general liability (CGL), directors and officers (D&O), errors and omissions (E&O), employment practices liability (EPL), business interruption, variable annuity, and other insurance policies. Bill earned the Chartered Property and Casualty Underwriter (CPCU) designation early in his career while working as in-house counsel for State Farm.

Room 120
1:45–2:45 pm

Does Anyone Remember Enterprise Security Architecture?

Rockie Brockway, Black Box

The concept of Enterprise Security Architecture (ESA) is not new (Gartner 2006), yet the numbers from the past several years’ worth of breach data indicates that most organizations continue to approach security on a project by project basis or from a compliance perspective. This talk will refresh the ESA concept and communicate tangible and realistic steps any organization can take to align their security processes, architecture and management to their business strategies, reduce business risks and significantly improve their overarching security posture.

BIO: Rockie Brockway is the Information Security and Business Risk Director at Black Box and a BsidesCleveland organizer. With over two decades in InfoSec/Risk, Rockie teams with clients to understand the value and location of business critical data in an effort to further enable organizational innovation and to protect the brand.

Room 127
1:45–2:45 pm

Cyber Tradecraft or Espionage?

Hank Thomas, Booz Allen Hamilton

Join a discussion of the journey of cyber intelligence from a military intelligence perspective and its application to commercial markets. Learn through vivid examples about cyber threats and impacts. Minimize your cyber risks by applying the cyber tradecraft and understand the criticality of espionage techniques for uncovering cyber threats.

BIO: Hank Thomas is a founding member and Executive Director for Booz Allen’s Cyber4Sight™ threat intelligence service. Cyber4Sight™ is a predictive cyber intelligence capability used by a variety of markets to include financial services, oil and gas, energy, technology, automotive, global manufacturing, and retail.

Concerned About Business Continuity?

Uptime Solutions Associates, Inc.
Call us to discuss your plans. (937) 237-3400
www.uptime-inc.com

Where many companies fall short with their business continuity strategies is power and cooling
Unresolved heat issues, improper power sizing, too many UPSes, lack of system flexibility.

Start with us. Our team can offer solutions that avoid downtime and disruptions—using the best solutions available: Liebert Power and Cooling from Emerson Network Power.

Uptime Solutions Associates, Inc.
www.uptime-inc.com
Building Better Business Cases with Quantitative Risk Analysis

Apolonio Garcia, HealthGuard

The next time you don’t get a security project funded, check your business case. What did your cost/benefit look like? Often costs are described in hard numbers, but benefits are much squishier. This makes it difficult for decision makers to compare. Learn how quantitative risk analysis can “solidify” your benefits.

BIO: Apolonio “Apps” Garcia is the founder and President of HealthGuard, an Information Security consultancy that specializes in the healthcare industry. Apolonio has over 15 years of IT and business management experience, including 10+ years practicing in areas of information security and cyber risk management.

The Physical Security Evolution: Bridging the Divide between Facilities Management and IT

Jeffrey Blair, Savvux

As the Physical Security industry (CCTV, sensors, access control) makes a belated transition from analog to IP technologies, professionals on both sides of the facilities management/IT department divide face growing pressure to efficiently protect corporate assets. This presentation, through case studies, explores the changing face of Security.

BIO: Following 7 years in IT Infrastructure Service and Support, Jeffrey Blair is CEO of Savvux and its award-winning ‘HawkEye’ software. The HawkEye Suite has been certified by global leaders in the Physical Security industry including leading video surveillance and sensor manufacturers.

Why Not Trust Your Hardware?

Dr. O’Hair, ATIC

This presentation discusses, at a non-technical level, the threat against computer hardware. Specifically, how hardware can be taken over or compromised. The well-known malware threat (viruses, worms, etc.) and data theft seen in the news every day isn’t the only danger out there. Perfectly safe and trustworthy software can be compromised by running on hardware that has been taken over. While the landscape is bleak, it is not without hope. I will also discuss some of the ways to fight back using trusted hardware.

BIO: Dr. O’Hair has worked in the Intelligence Community for 30 years. First, as active duty military, he led development of numerous trusted Intelligence, Surveillance, and Reconnaissance (ISR) systems. Upon retiring, he went in to teaching ISR technology and developed numerous courses in remote sensing and trusted systems. Additionally, he led the creation of a large multi-level secure facility and was responsible for all levels of security (physical and cyber).
YOUR NETWORK IS IMPORTANT TO YOU
and it’s critically important to us.

Does alignment of business, organizational and technical goals seem impossible to you?

Not to us.

Our team of experienced strategists can help identify the security solutions that best suit your business needs. We take the complexity out of the network, giving you the confidence that comes from proven, measurable results.

There is no ONE single solution to security, but there is ONE source for ongoing security guidance.

Visit our booth at the OISC 2015 Security Conference to learn more about Cadre and our fellow title sponsors:

Simplifying the business of security.

PNC CENTER
201 E. FIFTH STREET, SUITE 1800 • CINCINNATI OH 45202
888.TO.CADRE | WWW.CADRE.NET
The Gluu Server is like a router for authentication and authorization. It speaks multiple dialects of SSO, and can help an organization manage both inbound and outbound authentication and authorization requirements. The Gluu Server is very flexible. Through the use of “interception scripts”, system administrators can mold the Gluu Server to solve the exact access management task at hand.

Benefits

Single Sign On
The Gluu Server stack includes both a SAML and OpenID Connect Identity Provider which can be configured for single sign-on to any SAML 2.0 or OpenID Connect protected application.

B2B or B2C
Organizations frequently have different requirements to authenticate employees and customers. Usability is not quite as important to an employer — use our security or there is the door! For customers, usability is more important — sometimes the best authentication for customers is the one they never even see. Through the use of “interception scripts” written in Jython, the Gluu Server can support any authentication logic or mechanism you can script.

Directory Integration
The Gluu Server can act as a bridge between your existing identity infrastructure and your applications, leveraging user information across not only Active Directory, but any LDAP V3 directory.

Alternative To
Gluu can be use as a great alternative to several other access management tools such as Oracle Enterprise Single Sign-On, IBM Security and Access Management, okta, onelogin and CA Identity Manager.

Who is Using It?
OpenID, Yubico, Toshiba, Oklahoma State University, University of Maine, and DuoSecurity are some of the security-conscious organizations that trust Gluu with their mission-critical identity operations.

Features
It has been proven that the majority of significant data breaches are caused by weak passwords and phishing schemes. Using the Gluu Server, you can configure multi-factor and multi-step authentication to applications and call external API’s such as intrusion detection.

The Gluu Server provides an interface to centrally configure authentication logic for your organization. Often times the device and context of the authentication drive the type of strong authentication that is needed. Gluu’s flexible authentication architecture allows your organization to simultaneously implement any of the above solutions, or any solution by request, with correlating policy to implement each mechanism as appropriate for the specified situation.

This Gluu Server has more features and is easier to manage than commercial alternatives. This recipe includes some of the most widely deployed federation components: like the Shibboleth SAML Identity Provider, and some of the most cutting edge security solutions available anywhere: like the OX UMA Authorization Server.

For a library of Open Source software go to opensourceohio.net

As a pioneer in Open Source, Ardent Technologies has successfully deployed Open Source applications for government and commercial customers of all sizes across the country, delivering solutions up to 10 times faster and saving them millions of dollars in project costs.

Open Source Ohio connects graduates, students and displaced workers with small to medium size software development projects within local companies. Our extensive library of open source applications has been tested and certified by software development professionals.

Mark Wyatt from Ardent Technologies can be contacted at markwyatt@ardentinc.com.
Implementing Secure Software Development — A Method that’s Guaranteed to Work!

By: Max Aulakh, Chief Security Architect, MAFAZO Digital Solutions

If you ask enough people how and why a company was hacked, the answer will normally come down to few root causes. Two of the most common root causes of information security breaches today are humans and software related. Almost every aspect of a business today runs on software yet most software development activities do not include any software security engineering activities such as threat modeling or secure developer training. Most software is implemented without really thinking about how to build protection in from a cyber-attack perspective. Companies and systems will continue to be breached until humans are more aware of the risks and software security is completely baked into every step of product development. This includes products such as firmware that resides on all hardware devices to communication protocols such as IPv6 to enterprise applications, websites, mobile and desktop applications. It must be understood that no software can be 100% secure however, all software can be designed, developed and deployed in a secure manner much like a quality control process through implementation of a secure software development lifecycle (S-SDLC).

Secure Software Development

Most organizations today have a process for developing software, this process is customized based on organizations requirements and framework followed by organization. Secure software development introduces key input activities and steps that should be integrated into software development lifecycle in order to build secure and attack-resilient software. The graphic shows an example of a generic Software Development Lifecycle. The lifecycle provides a structured way to build software that completely caters to the needs of the end user. Software development teams employ various frameworks such as agile, XP or waterfall to move through this lifecycle quickly to deliver software. Secure development is about injecting appropriate security activities within these phases. The type of activities and frequency of activities heavily depends on the organization.

The Current Trend of Software Security Engineering

A customer has just sent you an email requesting to prove security of your application or to perform assessment of your software product. You forward the email to your security team to determine exactly what type of assessment will satisfy your customer needs. Your security team tells you about performing activities such as source code analysis, dynamic testing, threat modeling, and security requirements documentation and so on. You hire a 3rd party vendor to help you perform this assessment only to find out cost of assessment is much lower than the actual cost of fixing issues found. Your development team is frustrated because now you have just added hundreds of tasks to their list and potentially re-architecting components of the software. If this sounds all too familiar, you are not alone. This is the current approach to implementing security within software – it’s 100% driven by an external reactive force such as a regulation or customer, which are driven by industry attacks such as the Anthem & Target breach. This industry wide knee jerk reaction trickles down to your developers and you identify issues by performing 3rd party assessment of the application and then fix them in a much more costly and time consuming way or worst never address the issues.

A Better Way

Attacks will not stop and neither will new regulations that continue to raise the bar on issues related to consumer privacy and security of their data. Organizations who understand this are one step ahead of their customer requirements as well as a step ahead of hackers. Below are four steps to improve software security within your software development teams. This isn’t an easy task but if achieved properly can save an organization tremendous amounts of money and headaches.

Step 1: Establish a Case for Secure Development

Gaining management buy in is critical for your secure SDLC project to be successful. This requires understanding the business drivers for your organization which could be customer driven, cost avoidance, regulations or just general good business practices. Management buy-in includes a budget as well as policy level support. You will also need an internal champion to start implementing this change of process and influencing developer behavior within your software development teams. The best recommendation is to start with one development team versus trying to implement secure development blindly across the whole enterprise or within all your development teams. Start with a team where you understand their product, development culture and their challenges.

Step 2: Start with Training

Your initial investment must be in people over software security automation tools. There have been too many times where we have seen security tools purchased and never used properly due to lack of training or fundamental understanding of software security. Also, software security tools are so complex that it is best to first start with training. A great example of first course for your developers might be software security 101, .NET secure programming or Open Source Web Application Security Project (OWASP) Top 10 secure development training. It is important to note that the training you implement for developers must be specific and actionable, there is nothing worse than having to attend security training that is too general or not applicable for your developers. It might be best to try scheduling secure development training in small (continued on page 11)
doses such as lunch and learns on specific topics like covering injection attack for 1 hour with some real world example code from your own organization.

**Step 3: Integrate Security Activities**

Next step is integration of security activities within each phase your development lifecycle. This is tough to figure which activities makes sense for your environment because not all phases of the software development lifecycle are followed especially in agile development. In a fast paced development environment, requirements are sometimes developed during design or implementation and testing is conducted as your product is getting ready to be shipped. Our recommendation is to start with light activities such as threat modeling or security design requirements and then add more activities every cycle until it becomes natural for your development team. This will ensure that your development team doesn’t become overwhelmed. The goal here is to slowly change behavior of your developers to start thinking about security as their primary way of solving programming challenges. This is actually very tough to do because there is a normal resistance to change in adding additional tasks for the development team.

**Perform Selected Security Activities**

Microsoft lays out seventeen different security activities for Secure SDLC implementation. At first, performing security activities will feel clunky and out of place for everyone because it is something new for your team. But overtime, activities such as team threat modeling or source code analysis will become the norm. Your development team will figure out how to implement security better than your matrixed application security architect because they are more familiar with the product. Finding existing security flaws within the architecture or security bugs are great opportunities to teach and learn about security for your development teams. When you feel your team has mastered a few of these activities — add a few more that are different that challenges them to think differently about security.

**Rinse, Repeat & Learn**

There are very few organizations that get to the point where they are able to measure maturity of the development team from a software security standpoint. Therefore, secure SDLC involves a strong element of continuous improvement. As you learn more, you should implement more activities. If your development team is taking on a new product or creating a new feature, they should continuously take training on various programming language specific security issues to improve their understanding. The training does not have to be formal classes but more so lunch and learns or just simple 1–2 hour sessions on specific security topics that can be immediately applied within your development environment. A key part of Secure SDLC is creation of artifacts such as test results, design documents, etc... these documents are important to prove compliance. Also, these documents will help your 3rd party security assessment team to find problems that are not yet known instead of finding problems that are already documented. Automation tool for source code analysis or dynamic testing should be purchased only after your team understands how to do secure development to reduce frustration. These automation tools can generate compliance related artifacts for you.

**Step 4: Celebrate Results**

Secure development really comes down to great management of your development team. A good manager will always celebrate results like cost control and security defect reduction. Give your development team recognition because after all it is about changing behavior by teaching and rewarding than by ignoring and dictating security at the last minute. You will start to notice that team morale is up and developers are much happier by actually implementing this last step. This inevitably leads to retention of the employee because today good developers are very difficult to find and keep.

In conclusion, to start with secure development the right way be sure to get buy-in from the top management and also the bottom-up through your development teams. When the funding is provided be sure to spend part of your initial investment in humans over tools, your developers will respect you for it.

Article by: Max Aulakh, Chief Security Architect, MAFAZO Digital Solutions. Max can be contacted at max@mafazo.com or www.mafazo.com.
Physical Security and the Internet of Things

By: Kathy Vogler, PERRY proTECH, Marketing Director

When we talk about the importance of cyber security, we often focus on the Internet and the cloud. We understand the need for strong user authentication, event monitoring, activity logging, encryption of data and all of the controls that need to be built in to our IT networks to keep us secure. As the Internet of Things continues to grow (to an estimated 20 to 50 billion devices by 2020), we need to make sure our physical security is looked at with the same eyes too.

Physical security is the protection of life and property and includes things as diverse as people, hardware, programs and even the data that occurs from an event that causes loss or damage. Access control and video surveillance were built to perform very specific security functions: keep an eye on the good people and don’t let the bad people in. At first, these solutions were not connected to other systems and were purpose built and self-contained. CCTV systems had cameras linked through coax cable with proprietary communications to a video controller that sat in its own closet somewhere. Users had credentials like badges, tokens or fobs that connected straight to the identity and access management tool system. Equipment was monitored and serviced by facilities teams or outside contractors. Not the IT department.

A breach of the independent physical security solution could be carried out with little or no technical knowledge by the attacker. And, natural disasters and accidents are an inevitable part of our daily lives. But the Internet of Things and interconnectivity is having a big impact on the physical security industry. This brings two questions to mind; how do you connect physical security devices to the Internet and ensure they are protected from hackers and how can you use your current surveillance, access control and intrusion detection devices that are already in place? Older, out of support systems such as Windows XP may be a critical part of a physical security system that is now moving to the larger picture of the Internet of Things.

Our legacy and closed systems can only go so far, and at some point they can’t keep up with the massive amount of information. We all know an employee or two who found a work around to the systems — prop open a door, borrow someone else’s fob, wait until someone else gets access and slip in. And, when things didn’t go as planned (such as a reader malfunction) possibly had to stand outside in the dark or in the rain waiting for entry. And, this is where the The Internet of Things is a natural progression for security. The IoT offers a way to improve our physical security and access control systems. With the IoT and cloud management, we can use our existing solutions but improve on them with scalability and system changes that are shared across the network in real time. Systems will need to be open-sourced and available on multiple platforms, just like in network technology. Manufacturers will need to figure out how to serve this market. And, many traditional networking vendors are already working on open camera IP platforms that enable attachment to edge-based storage and offer an API for application development.

Connected devices and their inherent vulnerabilities add complexity to our network architectures. And just like BYOD came through to business from consumers as we brought our new personal devices to work with us, the consumer in each of us will expect everything to interconnect and that all of our devices should be able to speak to each other. Autonomous machine to machine data transfer may link our smart phones to our cars to our homes. The business technology network and our physical security systems will also have to figure out how to make all of that interconnectivity work. And stay secure. Security loopholes can occur anywhere in the IoT and new smart devices that often started as dumb (or non-connected) objects don’t always store sensitive data in secure locations. Sometimes the data goes into a collection hub and then gets uploaded in bulk. The OS, firmware and patch support that IT is accustomed to is not always available with these devices. In addition to the security of that data, who is watching out for the privacy? The IoT presents itself with great opportunity and even greater responsibility. Regulation and legislation will be difficult since we can’t predict where this will go or what will happen. But, it is certain and we can’t allow automated systems to interact with our physical world and possibly endanger lives.

What happens if the Internet goes down? You can bet our government is worried about what happens if the Internet is compromised — not just the surface web, but the deep web or the dark part that is just like a power grid. As the IoT consumes more (continued on page 13)

Success Depends on Unique Ideas

Taft’s attorneys focus on providing individualized, comprehensive legal strategies to meet our clients’ business goals.

www.taftlaw.com

Chicago / Cincinnati / Cleveland / Columbus / Dayton / Indianapolis / Northern Kentucky / Phoenix
and more devices it becomes just as impactful as power. All systems need redundancy and safe-check mechanisms. We can't rely on a single point of failure and need to think about the things that can go wrong and invest in those technologies.

A study by VMware found that fewer than one in four IT professionals are confident in the secure configuration of IoT devices such as Internet phones, physical security sensors, smart controllers for lights and air conditioning and point of sale units that are already on the enterprise network. The bad guys will take advantage of devices that are put online with default settings that allow anyone with web access to take control. Today we are seeing IoT devices ship with default passwords like “12345,” vulnerable services such as telnet enabled and firmware updates that depend on HTTP calls. The “Enterprise of Things” white paper shows that remote workers have an average of 11 Internet-connected devices on their home networks. Employees often download third party apps and then connect to the corporate network over a cheap home router. And, now with the interconnectivity, the attacker doesn’t just get into your data on the back end but might be able to walk right through your front door.

Companies with the most experience managing complex technology and physical security integrations will be the ones more likely to succeed in an IoT environment. Many of us felt the first impact with virtualization and cloud services and soon thereafter BYOD’s wave of disruptive technologies that also threatened our well-established security practices. The IoT brings a wide range of intentions and business purposes and can quickly lead to an exploding security minefield. The IoT is a convergence of your organizations existing information technology and operational technology networks and requires a new approach that combines physical and cyber security components.

---

**MEMBER MENTION**

**Company Recognized for Exemplary Approach to Delivery of Managed IT Services**

PERRY proTECH has earned recognition on The Channel Company’s 2015 CRN Managed Service Provider (MSP) 500 list as one of the MSP Elite 150. This annual list distinguishes the top technology providers and consultants in North America whose leading approach to managed services enables their customers to improve operational efficiencies, elicit greater value from their IT investments, and successfully leverage technology to achieve greater competitive advantage.

Coverage of the MSP500 will be featured in the February 2015 issue of CRN and online at www.CRN.com, Learn more about PERRY proTECH at www.perryprotech.com.
NEW JOB POSTINGS

Technical Lead ........................................... Ardent Technologies Inc
SharePoint Architect .................................. Ardent Technologies Inc
Voice Engineer ......................................... Netgain Information Systems

TECHNOLOGY FIRST BOARD OF DIRECTORS

Diana Bolden
Chief Information Officer
Teradata

Gary Ginter
Premier Health
System Vice President,
Chief Information Officer

John Huelsman
Director, Business
Support Services
Hobart Service

Dave Rotman
Associate Vice President
for Technology
Chief Information Officer
Cedarville University

Jim Bradley
Global IT Director
Symmetry Medical

Steve Hangen
President
The Entrepreneurs Center

Tim Hull
President
TDH Marketing/Bitstorm Web

Leigh Sandy
Founder
Extra Mile Fiber

Gary Codeluppi
VP, Marketing and
Business Development
The Ross Group

Barbara Hayde
President
The Entrepreneurs Center

Scott McCollum
Chief Information Officer
Sinclair Community College

Thomas Skill
Associate Provost & CIO
University of Dayton

Doug Couch
Vice President, Information
Technology Services
Speedway

Bryan Hogan
President / CEO
AfdenceIT

Monique McGlinch
Midmark Corporation
Vice President, Information
Technology and Customer
Experience

Diana Tullio
Chief Information Officer
Standard Register

Ann Gallaher
Chief Operating Officer
Technology First

David Hoskins
Director of IT Workflow
and Collaboration
CareSource

Paul Moorman
IT Strategist
NewPage Corporation

Jeff Van Fleet
President
Lighthouse Technologies, Inc.

Technology First would like to thank and recognize its Board of Directors. They provide input into the strategic direction of the organization and actively lead working committees that drive our programs and services.

Publisher: Technology First
Chief Operating Officer: Ann Gallaher
Managing Editor and Advertisement Sales: Michelle Marek

Design & Production: Courtesy of Bitstorm Web

Writers: Our mission is to support the growth of Greater Dayton's information technology industry. Technology First provides a forum for educators, business, and technical professionals to communicate their expertise and lessons learned while working in the field. Please submit the article in Word, preferably with 500 to 700 words, with any graphics in pdf to agallaher@technologyfirst.org. Please include your name, business organization, business address, phone number, fax number, e-mail address, and a brief description of any professional accomplishments. Please also include a digital photograph if available.

Subscriptions: Non-member business/home delivery of this publication is available at $120/year (11 issues). Mail name, address and check made payable to Technology First.

2015 Technology First; All rights reserved
714 E. Monument Avenue; Suite 106 • Dayton, OH 45402 p: 937.229.0054 www.technologyfirst.org
As the official training partner of Technology First, Sinclair Workforce Development provides relevant professional-level courses and support for training, certification and recertification, custom engagements and consulting.

Contact us today to learn about our upcoming training and development classes for 2015!

- SharePoint  
- Cloud Essentials  
- MS SQL  
- CompTIA A+, Network+ & Security +  
- Transitioning to Windows 8.1  
- MS Project (Levels 1 & 2)  
- AND MORE!

SINCLAIR Workforce Development
937.252.9787  workforce.sinclair.edu
Bring the World to Your Website

Go Mobile Responsive

Bitstorm Web builds brand awareness and generates new business leads through:

- Responsive Web HTML5 and CSS3 Development
- Custom Apps Development
- Ecommerce Solutions
- Search Marketing
- Social Media Marketing
- Content Management Solutions
- 3D Modeling and Animation
- Video Production

www.bitstormweb.com  937-438-3434  info@bitstormweb.com