Cyber-Security Essentials

for State and Local Government

□ Best Practices in Policy and Governance

□ Operational Best Practices

□ Planning for the Worst Case

Produced by Government Technology's public cio

with content expertise provided by at&t

For additional copies or to download
this document, please visit:
public-cio.com/security

The information in this document is provided by AT&T for informational purposes only. AT&T does not warrant the accuracy or completeness of the information or commit to issue updates or corrections to the information. AT&T is not responsible for any damages resulting from use of or reliance on the information.

Cyber-Security Essentials

for State and Local Government

Table of Contents:

CLICK LINKS BELOW TO SKIP TO EACH SECTION

Introduction

In recent years, IT security teams have had to contend with increasing numbers and sophistication of electronic attacks, regulatory compliance and a variety of new technologies coming onto the market. IT security teams are responding, but it takes buy-in from an entire organization to truly maximize the contributions from security personnel and systems.

In government, it's imperative for CIOs and other executives to understand the security threats, the technologies and the issues involved in keeping the IT environment safe from attackers. Executives need to know as much as they can about the challenges faced by their cyber-security teams.

This guide shares best practices for policy and governance, operations and worst-case scenarios. It addresses things like the importance of protecting not just the network, but also the systems, applications and data within it. It also covers topics such as getting IT security experts involved earlier in the life cycle of new projects and the need for strong policy and risk management. This guide also provides insight into security practices for three areas that are rapidly becoming more important in the current threat landscape: applications, the cloud and mobility.

It's important to create a better, stronger, more flexible approach to security now, because the challenges are expected to continue. Experts say cyber-attacks will continue to increase in the future and the rate of adoption of advanced technologies will certainly move at a faster pace.

SECURITY CHALLENGES

Today, protecting data is more critical than ever. Every organization has mountains of data, and hackers are going after it like never before. Instead of fame, cyber-criminals are now interested in staying under the radar and quietly stealing personal data and financial information.

Other factors also add to the complexity of the current security landscape. Employees are bringing their own personal devices to work and using them for work-related activities. Industry analysts have indicated that smartphone use has increased dramatically around the world. The blurring line between personal and professional technology is making it more difficult to secure all these devices, as well as the systems and data they access.

Data sharing and cloud computing initiatives are also on the rise, meaning that data and resources often no longer reside within an organization's own network. Increasing compliance demands and new breach notification laws are also having an impact on security. For all these reasons and others, organizations must constantly update their policies, processes and technologies.

« TO TABLE OF CONTENTS

MORE TO DO

The future promises more work to do. Cyber-attacks will likely become more elaborate and will require more effort to stop.

New technologies like 4G and Long-Term Evolution (LTE) will change things too. And there will be more technologies that we can't even guess at right now. More organizations may opt to work with outside providers to help them with security, thus bringing in experience and expertise they could never have on their own.

Increased funding for security and better employee training are vital. And as organizations strive for more efficiency and productivity, the need for security teams to work more closely with the business will be an important factor. The constantly evolving security landscape requires nonstop vigilance on the part of security professionals and the organization as a whole.

Cyber-security is a key part of providing mission-critical IT services. That is certainly the case today, and it will be in the future as well. Every person in an organization can help improve security, and IT security professionals must have all the tools necessary to lead that effort.

Government CIOs and other executives need to do all they can to help improve security. Understanding security best practices, the latest challenges and the needs of their security teams can help CIOs and executives lead their organizations' security efforts now and in the future.

« TO TABLE OF CONTENTS

Best Practices in Policy and Governance

Policy, governance and senior management buy-in are cornerstones for any information security program. The risk landscape is complex and fast changing. Thus policy and governance form the basis for managing risks as effectively as possible.

Strong policy and governance also can make an IT environment more efficient and productive. Breaches are costly, but so are inefficient processes that don't mesh with core business objectives.

When creating security policies, it's important to align them with business objectives. That includes making sure security measures are enabling the business, not hindering it. It's important to get buy-in from the business side of the organization. If all lines of business are on board with security policy from the beginning, and have input into the process of creating it, you'll have an easier time later getting everyone to observe the policies.

It's also crucial to have executive support for security policies. An organization's leaders have to be behind these policies if they are to be enforced and adhered to throughout the organization. Policy documents should be constantly refreshed as business structures change or new technology is adopted.

RISK MANAGEMENT

Risk management is about understanding how security events would impact individual assets and the organization as a whole. Effective risk management requires:

- Identifying your critical assets.
- Analyzing what threats and vulnerabilities could harm these assets.
- Understanding the implications of a security breach.

Risk management is also about evaluating your assets and comparing the cost of loss or replacement to the cost of protecting the assets. It also analyzes the likelihood of an attack or exploitation in comparison to the cost of preventing it.

Determine Your Risk Tolerance — Determine what your organization's risk tolerance is and what influences it. Some organizations are more risk-tolerant or risk-averse than others. Risk tolerance is determined by an organization's mission and culture, and by the legal or regulatory environment in which it operates.

Assess Your Business Needs and Relevant Risks — Be clear about your security objectives and how they align with your business objectives. Understand what your organization's risk appetite is. Prioritize security-related projects, and create a plan based on your risk exposure.

« TO TABLE OF CONTENTS

Have Strong Data Discovery — Before you can protect all your data, you need to know where all of it is. From both a compliance and risk management perspective, data discovery is becoming more important. Find out where your data resides. And look at more than just stored data; think about all the data in documents being e-mailed throughout the organization and to other entities. Do an accurate inventory of top critical business systems and environments. Find out which systems are connected to them and what the potential impact to other critical systems and operations would be if any of those systems were compromised.

Standardize Risk Management — Have a common yardstick for measuring risk across all the divisions within your organization. It's harder to make security decisions when different departments view risk differently. Create a risk profile that's unified across the organization.

COMPLIANCE

Organizations need to comply with numerous government laws and regulations. These can relate to the care and protection of health-care information, credit card numbers, Social Security data and other personal information of citizens. Many states have enacted breach notification laws requiring that citizens be informed if their personal data is compromised.

To ensure the confidentiality, integrity and availability of your data, put as much effort as possible into meeting your compliance obligations. Assess where your organization stands on compliance, and move forward. Many organizations find that once they study their compliance situation, they see opportunities for improvement.

RESOURCE:
The **Governing for Enterprise Security Implementation Guide** provides best practices for IT security governance. This is a publication from the Software Engineering Institute at Carnegie Mellon University. www.sei.cmu.edu/reports/07tn020.pdf

Control Three Areas — Technical, administrative and operational controls are all crucial to meeting compliance requirements. Your systems, your policies and your people must all complement one another and work toward the same compliance goals.

Bring in an Expert — Have an objective expert assess the compliance risk for your environment.

Budget for Compliance — Too often, organizations spend money on new equipment to expand services or capabilities, but they don't put enough into the proper tools for compliance. When budgeting for new initiatives, include funds for compliance.

Review Activity — Review system activity records on a regular basis. These can include audit logs, access reports and incident reports. Focus on compliance, and shore up any weaknesses.

« TO TABLE OF CONTENTS

EMPLOYEE TRAINING POLICY AND PROGRAM

An organization's workers don't always know which links they shouldn't click on, which are safe to open, what devices they shouldn't connect to their computer or how to use a mobile device in the most secure way.

Significant breaches have occurred thanks to breakdowns in basic security principles. A strong training policy and program can help your organization keep its environment secure. Attacks have evolved over the years. Today many attacks aim to trick people into helping perpetuate them. Employees must be made aware of your organization's security policies and how to safely use devices and systems that connect to your network.

Make Training a Priority — Government budgets are tight, but employee security training is worth the expense. A security breach can be costly in many ways, and employees are often unintentionally responsible.

Build the Culture — Try to get security on everyone's mind. Posters, signs, e-mail blasts and other messaging techniques can help raise awareness. Recognizing and commending staff that abide by policies can also help get employees thinking about security.

Get Employees on Board — Make sure employees understand why there are security policies. Don't just tell them what to do and leave it at that. They're likelier to observe policies if they understand the reasoning behind them. Give them examples of how security could be compromised if they're not careful.

Provide Solutions — Sometimes employees compromise security by using consumer-driven tools that aren't up to your security standards. For example, they might use a file-sharing website because it helps them be productive. If you build a similar solution in-house or direct them to a third-party solution that meets your security needs, you can give employees the tools they want and also know that the solution is secure.

RESOURCE:
TechRepublic is a website focusing on a variety of IT matters, including IT security policy and governance.
www.techrepublic.com

USE OF NEW TECHNOLOGIES

Traditionally when lines of business want to do something new with technology, the security team has acted as gatekeeper, raising a red flag about potential security issues only upon learning, sometimes late in the process, of the business's plans. The people focused on the business of the organization don't typically think of security at first. Try to change this mindset — especially when it comes to new technologies.

Get Out in Front of Emerging Technologies — Security should be as prepared as possible to hit the ground running when new technologies become available. Stay ahead of the curve on architecture, user agreements, policies and more.

« TO TABLE OF CONTENTS

That way, security can give other departments the go-ahead to use the latest technologies right away.

Revisit Policy — Review policies often, and make revisions that keep things secure while also helping the organization achieve its goals — even if they're evolving.

Beware of "Consumerization" — While employees bringing their consumer-driven devices to work can aid their productivity, most employees aren't aware of the security risks that come along with them. You need a security policy that covers these.

Address New Technology Periodically — New technology should be part of the overall risk assessment process. It should be re-evaluated annually.

MEASUREMENT AND REPORTING

You need policies for what gets measured and reported on in your IT environment. It's likely that many security elements within your network and IT infrastructure can capture data. How much of it do you look at? Policies should govern all measurement and reporting activities.

Align With Critical Business Goals — Look at your goals and how security can enable reaching them. Then create metrics that help your organization keep security and operational goals aligned.

Create Metrics Wisely — Some organizations make policy statements that are difficult and costly to measure against. Make sure your policy doesn't require gathering metrics that are unrealistic to collect. Also, make the process as automated as possible.

Make Reports Easy to Understand — Some metrics are only understood by security experts. Others are easily understood by a wider audience. Think about who will be reading the reports and aim them at the target audience.

Use Metrics to Improve Security — After capturing and analyzing your measurements, use data to refine your existing security program.

CHECKLIST — POLICY AND GOVERNANCE

- □ When planning new projects, get IT security involved at the beginning.
- □ Make sure all lines of business are on board with security policies.
- □ Standardize risk management across all divisions.
- □ Assess where your organization stands on compliance, and make appropriate changes and improvements.
- □ Help your employees to understand the reasons behind your policies — not just what to do/not to do.
- □ Make sure your security metrics are aligned with critical business goals.

« TO TABLE OF CONTENTS

Operational Best Practices

Cyber-attacks occur every day. By taking security seriously, and adopting best practices and sticking with them, organizations have a much better chance against attackers — who are constantly seeking new vulnerabilities to exploit.

Operational best practices for security protect against the latest threats and enhance any necessary mitigation. They can also help to streamline the security environment, thereby increasing operational efficiency and reducing costs.

Network and IT Infrastructure Security

The importance of keeping your network and infrastructure secure cannot be overstated. Viruses, worms, Trojans, botnets and other malicious forces can strike just about any organization without warning. The bad guys don't rest, and they succeed if strong security is not in place.

A successful attack can cripple a network, compromise sensitive data, attract negative publicity and be costly to remediate. It could lead to fines and civil lawsuits. Guarding your network and IT infrastructure requires vigilance.

Assess Your Needs — What are the goals and objectives for your network? That will help determine what types of security you need for the various parts of your infrastructure. It will also help you spend wisely and get the most benefit from the money you put into security.

Assess Your Current Infrastructure — How well are things working? How could they perform better? What security improvements are needed? Be sure to know where communications are occurring into and out of the network. Many organizations are surprised to learn just exactly where network communication is occurring. Consider having an independent third party perform a formal risk assessment. Internal efforts often get no traction.

Classify and Evaluate Data — Data classification helps define what data you need to protect and how. Different types of data require different levels of protection. To protect the various levels properly, conduct a thorough data classification and define your needs.

Correlate — Correlation tools give you better visibility into what's happening on the network. By comparing alerts or notifications from multiple sources within your network, you can see relationships you wouldn't be able to detect

« TO TABLE OF CONTENTS

otherwise. Events that might seem unrelated when viewed in isolation reveal more information when they're correlated. For example, you can determine that an event happening on one side of a firewall is related to something happening on the other side — which could mean a security breach.

Evaluate Security Infrastructure for a Move to the Cloud — Cloud computing continues to expand, and with good reason. It's efficient, cost-effective, flexible and easier to manage than traditional computing. It also leverages virtualization, another hot technology that's popular because it works so well in so many ways.

Numerous security processes can be moved to the cloud. Look at your systems and see what you might be able to move into a cloud environment. Good candidates include e-mail security, Web security, firewalls, distributed denial of service (DDOS) protection, intrusion detection systems (IDS) and intrusion prevention systems (IPS). The cloud can improve security processes and help you centralize security policy and implementation.

Security in the cloud can catch problems before they reach your network. If you go with a cloud services provider, make sure they have security features that can keep attacks far from your infrastructure.

Many organizations acknowledge that today's threat landscape is so dynamic and complex that it's difficult to keep up. By pushing security to the cloud and choosing the right partner, you can work with a provider that has much more insight into the threat landscape than you could ever have on your own. A good provider can detect and respond to threats more quickly than an organization that doesn't have security as its core competence.

The cloud can also help you standardize security. Legacy environments are often complex, with disparate systems that have been pieced together over many years. A move to the cloud can help you put more systems on the same platform. It also can improve correlation capabilities, providing a more in-depth analysis of security data. It gives you greater visibility into the network.

The cloud can also simplify security processes. For example, a major patch for firewalls that needs to go to 100 locations can be time-consuming and expensive if done the traditional way. It's much simpler to apply the patch to a single, virtualized system in the cloud, so you have better security and lower maintenance costs.

E-MAIL SECURITY

Hackers, phishers and other attackers constantly target e-mail systems and other messaging systems, such as instant messaging or social networking. Spam, Trojans, worms, malware and botnets are just a few of the threats to e-mail. Links within e-mails, if clicked upon, can download malicious content to the user's PC and network.

« TO TABLE OF CONTENTS

An e-mail/messaging security solution should handle all this and more. And it should support an organization's continuity of operations needs, in case e-mail ever goes down. It should also monitor both inbound and outbound messages.

Strong e-mail security should protect sensitive data such as credit card numbers and Social Security information, and it should prevent employees from accidentally sending this information out via e-mail.

E-mail security should help your organization stay compliant with necessary regulations. It should also improve your ability to archive and observe the appropriate e-mail retention guidelines.

Encrypt Messages as Needed — E-mail encryption is getting more attention from organizations that really want to protect their data. A good encryption policy is important. Encryption can be transparent to the end-user, users can encrypt things on demand or a combination of encryption practices may be implemented.

Look at DLP — Data loss prevention (DLP) focuses on monitoring and protecting data, both at rest and in motion. An organization's data is a valuable asset, and it must be protected in e-mails, in storage and as it moves over other parts of the network.

Employ Disaster Recovery for E-Mail — If e-mail is down, an organization's activities can grind to a halt. It's imperative to have backup capabilities in place, whether it's in-house or through a provider.

Consider the Cloud — Putting e-mail security in the cloud can have several advantages. You can catch issues far from your e-mail servers. It keeps traffic off the network, frees up bandwidth and reduces the processing load on your servers. These things all improve the efficiency of the network while providing better security.

WEB SECURITY

You can't control what's on the Web, but you can control what comes from it into your organization. To do that, you need solid Web security that protects against Internet-borne threats. Spyware, viruses and other threats abound. Proper Web security scans inbound and outbound traffic, blocks websites you want to avoid and keeps Internet access available.

Good Web security takes content filtering that was traditionally done at every separate location having a firewall and places it into the core network infrastructure instead. Like e-mail security and other functions, Web security can work really well in a cloud-based approach.

Web security should do category-based filtering, where it can strip out major categories of things that would have no business value, or content that is

« TO TABLE OF CONTENTS

inappropriate for a workplace. And of course, you want to keep out items that can adversely affect the network.

Use Automated Vulnerability Scanners — These can scan entire websites for vulnerabilities. Be sure to prepare carefully. Check settings and make sure the tool is tuned for optimum performance on the website you're building or maintaining. If you skip this step, the result will be false positives and other data that's a waste of time. If you prepare properly, you'll get more useful results. Many organizations combine this with manual penetration testing.

Get a Granular View — Your security system should give you granular control. You should be able to black list or white list exceptions to filtered categories — giving you more specific control over what can come onto your network from the Web.

Have a Social Media Policy — Social media sites can provide easy-to-use, cost-effective tools to keep citizens engaged. But it's wise to have some protections in place. Too often, government agencies adopt social media and Web 2.0 tools but don't have the same security policies and tools in place as in more traditional areas. Unfortunately social media can allow in hackers and other threats. If employees are too relaxed about social media and click on the wrong thing, the organization's entire network can be compromised.

STORAGE/DATA LOSS PREVENTION

There are many ways to secure data stored on servers. DLP is one layer. The majority of data that's lost leaves the organization via e-mail connections. By monitoring e-mail, and placing DLP tools there, you can identify when data is being released outside the organization — either purposely or inadvertently.

Security information and event management (SIEM) services from a third party can also help. Such a service should be able to do correlated analysis across multiple devices. So if a certain user is behaving differently than they usually do — perhaps logging into 15 servers from four different locations when they're typically on five servers from one location — alarms will be triggered. But such behavioral shifts will only be noticed if a security system is looking for these types of things.

Prioritize — In addition to the data itself, there are other things to consider. You need to keep in mind a variety of factors affecting data and storage security. These factors can include past breaches, the amount and type of communications your

« TO TABLE OF CONTENTS

organization engages in, number of users, and likelihood of a future breach. Once you look at the big picture, you can prioritize next steps for DLP.

Take the Extra Step — For a long time, a typical approach was to secure the network and then assume the data inside it was also secure. Now organizations realize that's not good enough, and they're taking extra steps to secure the data as well. Identify, classify and protect the data appropriately.

Protect Data at Rest, In Motion, In Use — Basic protections, such as firewalls and IDS, protect your network and the data traversing it. DLP, encryption, redundancy and network-wide correlation can all help protect data when it's not moving across the network. Make sure you have a highly resilient storage environment that's scalable.

MEASUREMENT AND REPORTING — LOGS

There are basically two types of measurement and reporting. One is for performance, and the other for security. You must have the right tools in place to identify threats and send the proper alerts for security issues within your infrastructure. By measuring network status against security thresholds and reporting on the issues, a good security system can help you avoid trouble. This can also tell you where you need additional capacity or where the network is stressed.

See Into Your Network — Having proper visibility into your network is one of the most important things you can do for security. For example, if your endpoints are connecting to some overseas location they shouldn't be, you need to know that. You need to have the tools that allow that visibility.

Feed Data Into a Correlation Engine — Data logs from all critical pieces of network equipment should be fed into a central correlation engine. This should serve not just to collect the data, but also to report on it. The system should collect disparate data from across the organization and do proper correlation, so it can give you actionable alerts. For example, a stealth attack — one that's disguised to look like normal activity — can be very hard for a piece of equipment to recognize on its own. But with correlation, it's likelier to be discovered.

Analyze — Collecting security information is one thing, but being able to build the algorithms needed to properly analyze the data is another. For many, outsourcing the work to a provider makes sense. They have the experience needed to look for

« TO TABLE OF CONTENTS

certain types of anomalies within huge amounts of data and can turn that into actionable information for you.

Vulnerability and Threat Management

Vulnerability and threat management requires continuous monitoring, collecting and analysis of security event data. It's about knowing your infrastructure well, and knowing what attacks could do it harm. It's looking at trends and identifying new types of attacks.

Proper employee training, careful authentication and authorization of those using your network and resources, intrusion detection and prevention, and defending against DDOS attacks are all essential measures that help keep your network safe and healthy.

EMPLOYEE TRAINING

Employee training should be a key part of an organization's risk awareness and prevention efforts. Employees should know what the risks are and what to do to prevent security compromises. No matter what attackers are doing, you have a better chance at defeating them if all employees are in on the effort.

Compliance guidelines are driving more organizations to step up their training efforts. That's good not only for compliance, but also for improving security in general.

Have a Living Document — Don't just write a training document and forget about it. Keep it updated. Make sure it accurately describes today's security policies.

Educate — Make sure you have formalized, structured training. And make sure it actually occurs. Too many organizations have employees sign the security policy once a year, without ensuring they comprehend the information. Make sure people understand things like phishing attacks, scams and what not to click on. The best training doesn't just tell people what they can and cannot do, but educates them as to why.

Address Social Media — Social media is playing a larger part in government. Unfortunately it can also be a way to distribute malware. Make sure if employees use social media, they're doing so according to your policies, and not the policies they observe in their personal communication.

ACCESS, AUTHENTICATION AND AUTHORIZATION

Access, authentication and authorization processes allow you to decide which groups or individuals can connect to and use specific resources in your environment. You typically don't want a policy that lets everyone use everything. Access, authentication and authorization allow the right people to interface with the proper segments of the network, the right servers and the appropriate data.

« TO TABLE OF CONTENTS

Have Strong Password Policies — Make sure employees know why password policies are important. Make it clear to employees what makes a good password and what doesn't. Make sure people change their passwords on a regular basis. And it may sound obvious, but it's important to remind employees not to write their passwords on paper that's accessible to others. A good solution can be single sign-on, which is simpler for users, saves time and gives the opportunity to make security stronger at one key point instead of duplicating sign-on security in several places.

Use Two-Factor Authentication — Don't settle for just a username/password; require users to have something extra, like a security token.

Consider Biometrics — A new type of authentication is biometrics, which can use voice, fingerprints or facial recognition to ensure users are who they say they are. Biometrics add an extra level of security, and it's convenient for users.

Have Proper Network Access Controls — With the proper controls, you have more power over who can connect to the network. For example, you should be able to ensure that users wanting to connect have updated their own security with the appropriate patches and updates. If they're not current, you can block them from gaining access.

Hold Third Parties to Your Standards — Any third parties connecting to your network should be held to the same security standards as your own people. This should be the case especially if you're sharing data.

Have Interface Agreements With Third Parties — These contracts should spell out exactly what kinds of security standards must be observed by vendors, suppliers and other third parties you connect with.

INTRUSION DETECTION/PREVENTION

Intrusion detection systems and intrusion prevention systems, along with firewalls, form the basic security against cyber-threats. They are typically supplemented with other layers of protection. These systems generate data which are most often useful when correlated with other types of data from the network.

Tune IDS — It's important to get your IDS tuned properly, so it's only calling out legitimate threats and not generating too many false positives. It's also important to place sensors — the applications or devices set up to catch inappropriate activity — in the optimum positions throughout the network. Putting sensors in the appropriate places will generate more actionable information.

Be Careful With IPS — Few organizations use IPS in active mode. It's more commonly used in passive mode so it can search for anomalies and

« TO TABLE OF CONTENTS

behavior that could be attacks without being too aggressive and slowing down network traffic.

DISTRIBUTED DENIAL OF SERVICE PROTECTION

DDOS defense is critical. That's because hackers have become more adept at commanding armies of "robot" computers they've managed to infect over time. These botnets can suddenly bring down a website, leading to disappointed and angry constituents and plenty of negative publicity for the targeted organization.

DDOS attacks are becoming more prevalent, and the media has reported on numerous successful high-profile attacks. There are a variety of reasons for this kind of activity. Some groups bring down websites for political reasons. Even a relatively small botnet of less than 1,000 computers can cause big problems, and many botnets are made up of many thousands of infected computers.

DDOS attacks are easy to launch. Toolsets are sold on the Internet that can help people initiate them. Cyber-security experts agree that botnets are becoming more of a problem.

Get a Solid DDOS Partner — The best defense is a partner with specialized tools and expertise. The distributed nature of the attackers makes it very difficult for most organizations to see it coming. Sophisticated algorithms are needed to identify and mitigate a typical DDOS attack. If you rely on your own defense on your premises, by the time the botnet is recognized, it's already in your network.

Don't Become a Bot — You don't want to be the target of a botnet. You also don't want to become part of one. You want your computing resources to be used for your own purposes, not for those of the hackers. This is another reason to have good security in all areas of your environment — so attackers can't use your resources to do damage to others.

Application Security

Network and hardware security are fairly well understood, but that's not so true of application security. With the speed at which new applications are being released, especially for mobile devices, it's important to understand how to ensure security of the applications your organization uses. Web applications too are worthy of attention, as more and more citizen services are Web-driven.

Application security will become even more important as more computing moves into the cloud, since cloud computing is essentially driven by applications. And virtualization technologies are basically applications as well.

Sometimes application security is harder to grasp than traditional network or perimeter security; you can't grab a wire

RESOURCE:
OWASP (Open Web Application Security Project) is a nonprofit organization focused on improving application software. Its mission is to make application security transparent so people and organizations can make informed decisions about application security.
www.owasp.org

« TO TABLE OF CONTENTS

in your hand and trace it to a firewall. You can't put your hands on an application or see it, the way you can with other elements. Application security is more about process. And it crosses a lot of verticals within an organization.

Consider Threats in Context — The key threats to be concerned about for application security will vary from organization to organization. Do your applications process things like personal data or credit card information? Are they Web applications exposed to the Internet? Are they available to third parties? Assess the context around which your applications are used. That will help you determine where you may have security gaps that need to be addressed.

Follow a Life Cycle Process — Have a well defined set of security requirements. Make sure your security needs are understood by your developers and by third parties you're outsourcing development work to. Document all exceptions. Make sure you're tracking results. Go through quality assurance testing.

Think Security in Development — As with many types of security, application security should be baked in from the beginning. Developers should follow security best practices. They must understand application security and make sure they're building the proper protections into applications from the start. Security especially needs to be taken into consideration when engaging in custom development. Make sure developers scan code as they go; there are several scanning tools they can use.

Scan Often — Application scanning activities can also occur in software that's already been deployed. It's a good idea to scan monthly or quarterly, and also when changes are made.

Get Assessments From Third Parties — Make sure your developers aren't the only people looking at the security of the application. Impartial third-party penetration testing is a good technique to find vulnerabilities before the application is released for production. Consider teaming up with other agencies or departments to test each other's application security; this can be a useful, low-cost method.

RESOURCE:
The PCI Security Standards Council is an open global forum founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa. The council is responsible for the development, management, education and awareness of payment card industry standards, including standards for security. www.pcisecuritystandards.org

Put App Controls Into Infrastructure — As applications are deployed, place Web application firewalls and other controls into the infrastructure. These can give real-time awareness of attacks against applications.

Update Applications — Keeping up with application patches is very important — both for custom and out-of-the-box applications.

Engage Procurement — Make sure the procurement team is applying the same standards you use for application development to the application purchasing

« TO TABLE OF CONTENTS

process. Use purchasing agreements that require vendors to demonstrate compliance with security best practices.

Leverage the Broader Organization — Don't rely solely on your security team. Let purchasing, development, auditing and other departments contribute to the security effort. Keeping security on the minds of everyone can be beneficial in general. The bad guys work together to get in. Work together to keep them out.

Know the OWASP Top 10 — The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving application security. Every year, OWASP publishes information on the current top 10 risks associated with the use of Web applications. It makes the information available to the public, free of charge.

Cloud Security

Many government organizations are rushing to get into the cloud. The federal government has championed a cloud-based approach, and there are many convenient ways to get started, including everything from software as a service to infrastructure as a service. The cloud can be used for storage, applications and much more. There are private clouds, public clouds and hybrid clouds.

RESOURCE:
The Cloud Security Alliance is a nonprofit organization that promotes best practices for cloud security. It also provides education on the use of the cloud to help secure other forms of computing. https://cloudsecurityalliance.org

But organizations should take time to study how the cloud will be used, and consider the risks. The cloud is a unique environment, and organizations must have a solid security plan in place before venturing into it. Cloud resources are available via the Internet, so the ports into them can become a pathway for attackers. The fact that your resources and data are in a virtual environment that's shared with others is also a concern.

Cloud computing provides pooled resources that are accessible over a network on a self-service, on-demand basis, with rapid elasticity. Cloud computing is often enabled by virtualization technologies. The flexibility of these two technologies allows for very quick scaling up and down as needed.

Practice Risk Management — Different organizations have different levels of risk tolerance. If you're using the cloud to provide a portal for citizens to access government data, that requires one type of security. The security approach will be quite different if you're using the cloud to store sensitive citizen information. Look at the risks based on what you will do in the cloud.

Consider What Belongs and the Security Required — A lot of things can work really well in the cloud, including applications, backup systems, storage, e-mail and Web serving. But not everything belongs there. Consider security concerns when deciding what to put in the cloud.

« TO TABLE OF CONTENTS

Encrypt Sensitive Data — Because the cloud is a shared space, you may want to be extra careful with sensitive information. The cloud is potentially accessible to a lot of different entities. Encryption gives you more confidence that your data is secure.

Think About Location — If your cloud services provider is in another state, make sure the provider is observing your state's laws when it comes to securing sensitive data.

Put Security Requirements Into Cloud Contracts — Make sure the cloud service provider can demonstrate compliance and will keep security up to the levels you require. Make sure it's all in the contract.

Ask a Lot of Questions — How is data protected? How separate are you from other entities in the same environment? If others in the same environment have security issues, can those affect your services? Analyze the security posture of your cloud provider from an application/data-centric view. Use a cloud provider that has solid application security in place, including application life cycle management.

Add Additional Layers as Needed — Some organizations, depending on their goals and needs, choose to add layers of security for extra protection. These can include more stringent authentication methods or stronger encryption, for example.

Connect the Clouds — With more elements moving to the cloud, eventually clouds will need to connect to other clouds. Perhaps you'll have an internal cloud for core operations, and a backup cloud through an outside provider. Or maybe shared services make it logical for you to connect your cloud to that of another agency. Many scenarios are possible. Before leaping in, find out whether cloud technologies will be compatible with one another. Look into security risks that could result from connecting.

Consider a Consultant — Any good cloud service provider will want to ensure that the cloud works well for you. If the provider has a consulting division to help you make the most of the cloud solution you're purchasing, it may be helpful to include consulting support.

Mobile Security

The mobility landscape today is rapidly changing. Employees are using, or requesting to use, personal devices at work. People are paying for things with their smartphones. LTE and 4G are ready to increase bandwidth and speed. These changes present new challenges for security.

Two years ago, endpoint security would have focused on laptops. Now it has to include smartphones, tablets, removable storage devices and more. With today's

« TO TABLE OF CONTENTS

non-stop proliferation of mobile devices — and people depending on them more every day — endpoint protection is more important than ever.

As the numbers of devices and operating systems have increased, so too has the complexity involved in keeping them secure. And because smartphones are small and portable, they're often lost or stolen.

More organizations are allowing employees to use their personal devices to be more productive on the job. The technology provides robust connections and computing power, so a smartphone is essentially a floating version of the organization itself. So how do you keep the environment secure?

Organizations must develop new policies that cover such questions as, "Which apps and services are allowed? What does the organization pay for? Which operating systems will the organization support?"

Smartphones are also attracting the attention of hackers. Mobile botnets are a major concern. Advanced botnets can seek, destroy and steal data. Unprotected smartphones are often the entry point. Smartphones can be infected with viruses or worms sent via e-mail or compromised applications or websites. This can lead to automated attacks on the network. And 4G will bring greater speeds at which hackers can do damage.

RESOURCE: **SearchMobile Computing** is a website that presents a wide variety of information on mobile computing. Much of the information relates to mobile security best practices. http://searchmobilecomputing.techtarget.com

The mobile environment is likely to be the "next frontier," where all kinds of new threats will be unleashed. Vendors are working on new architectures and security approaches that can put most of the device security into the network, where organizations have greater control. Meanwhile, there are several best practices to consider.

Create a Unified Policy for Wired and Wireless — You want your wireless environment to be just as secure as your traditional, wired one. You should have consistent policies for both. You should also avoid having different policies for various devices, such as laptops, desktops and smartphones. Having one consistent policy across devices and operating systems simplifies management of security and also reduces the chances of a breach.

Use Mobile Device Management (MDM) — Management tools are essential for control over the integrity of smartphones, downloaded applications, and data accessed and stored on mobile devices. MDM software monitors and secures mobile devices, giving an organization greater control over smartphones, laptops, tablets and more. MDM can include encryption, and application detection and revocation. MDM can also help with phones that are lost or stolen, locking them down, wiping

« TO TABLE OF CONTENTS

them or setting off alarms. It also helps enforce policies. With the power to set and enforce these policy controls remotely on an enterprise-wide fleet of devices, you can worry less about hackers that “jailbreak” a device to download and run unauthorized applications, as well as employees who inadvertently download harmful content.

Control Applications — An emerging area of concern for security experts is the need for application controls. A growing number of stores are providing applications for mobile devices. This is another opportunity for malware to be distributed. You should have the ability to inventory the applications on devices. You must also ensure that security data from devices can be fed into a correlation system. Generate security logs just like you do for traditional IT equipment.

Centralize Network Traffic — Have IP traffic from smartphone devices flow into one centralized location for inspection and cleanup. For example, if malware, such as a bot, begins an attack on a smartphone, network administrators can receive alerts as the bot attempts to make its way through the central gateway. At that point, the network security team can mitigate the attack before it proliferates across the organization. A central gateway for all mobile-related Internet traffic enables central control for policy-based routing. The central gateway will also gather security intelligence from all smartphones or devices accessing the organization’s resources. With this centralized traffic management and the aggregated, documented security information gathered, you can proactively mitigate and manage mobility risks. You can also better monitor compliance with requirements for things such as the Health Insurance Portability and Accountability Act (HIPAA) for electronic health records and the Payment Card Industry Data Security Standard (PCI DSS) for credit, debit and other payment cards.

Think About Standardization — One approach might be to let employees bring their own devices only if they choose from a small list of devices the organization is willing to support and allow onto the network.

Consider a Consultant — Because today’s mobility landscape is fairly new and changing so rapidly, it might be beneficial to bring in an expert who’s steeped in the latest security methodologies for mobility.

Prepare for 4G and LTE — The higher bandwidth that comes with the next generation of wireless technologies will speed the flow of information. But it will also attract hackers. Be ready for new challenges.

APPLICATION SECURITY FOR MOBILE DEVICES

Applications for mobile devices require additional best practices. With many users bringing their own personal devices to work, organizations must be extra vigilant with their employee training and policies. Keeping personal and work data separate and secure is a big challenge. Users should be careful not to

« TO TABLE OF CONTENTS

download malicious content on their personal device when they have work data and applications there too.

A key strategy is to hold mobile applications to the same level of security as desktop applications. And because mobile applications are consumer-driven, many best practices for mobile application security are related to buying and using the applications.

Only Buy From Reputable App Stores — If you buy apps from non-official stores, you could be asking for trouble. Reputable stores are likelier to vet their apps, or ban malicious or poor quality apps they become aware of.

Load Only Apps You Need — Mobile apps are so easy to load, many people put them on their devices even if they don't really need them. Every new app is a potential security risk. Think of it as a numbers game. The more apps you put on a device, the more chances there are for things to go wrong. Choose only the ones that will bring real value.

Run Anti-Malware Protection — This is especially important if you do buy apps from non-official stores. But it's also a good idea even if you only buy from reputable stores.

Keep Apps Up to Date — It's easier than ever to update apps these days. It's an important security measure because updates usually include patches that fix vulnerabilities.

Get Rid of Apps You Don't Use — Apps that haven't been used in a long time can still be running in the background on your device. They could be performing functions you don't know about, or they could be vulnerable to attacks — especially if they're out of date or overdue for security patches. If you're not using it, get rid of it.

CHECKLIST — OPERATIONAL BEST PRACTICES

- □ Assess what you have within your network, and your goals for it. Then assess what you need for security.
- □ Make sure your development team understands security and makes it strong from the beginning.
- □ Protect not just the network, but also your data. Use encryption where it makes sense.
- □ Make security a big factor as you consider moving into the cloud.
- □ Hold mobile applications to the same security standards as you do desktop applications.
- □ Train employees well. Make them a big part of security efforts.
- □ Make sure you have up-to-date security policies for employee-owned devices used at work.

« TO TABLE OF CONTENTS

Planning for the Worst Case

Most government organizations realize they should prepare strategies to deal with security incidents. Experts agree that the prevalence of cyber-crime makes a breach more than just a possibility; they consider it all but a certainty. High-profile breaches exposing confidential data are reported on the news with alarming regularity. And while those reports are anecdotal, evidence exists to support the claim that electronic data is more susceptible to compromise than ever before. According to a recent study by the Ponemon Institute, cyber-attacks are getting more frequent and more sophisticated, resulting in more collateral damage.

Along with the growing impacts of cyber-crime is a fundamental shift in the types of crimes taking place. In the past, individual hackers took pride in their ability to expose vulnerabilities in the computer systems of high-profile organizations. Their primary aim may have been nothing more than bragging rights. But today, overseas groups are increasingly organizing large-scale attacks on digital assets to steal confidential personal information and intellectual property. The market for these illegally obtained assets makes them a lucrative commodity.

The average time it takes to effectively address any kind of technical breach is several days longer than it was just a year ago. In addition, the cost of breaches is on the rise. Aside from the loss of credibility and trust on the part of an organization's constituency, there are many other tangible costs, including data loss, lost productivity, damaged equipment, remediation costs, loss of availability of services to citizens and more.

RESOURCES:
The **Ponemon Institute** conducts independent research on privacy, data protection and information security policy.
www.ponemon.org

The Online Trust Alliance Data Breach and Loss Incident Planning Guide includes advice on creating an incident response plan.
https://otalliance.org/resources/2011DataBreachGuide.pdf

INCIDENT RESPONSE PLAN AND PROGRAM

Compliance guidelines for electronic resources require a detailed, tested incident response plan (IRP) to prove that public-sector organizations have laid the necessary groundwork for a timely, thorough and effective incident response. Requirements for an IRP vary depending on the nature of the agency. Variables such as agency size, type of services provided and degree of public contact influence what it should look like.

Adequate preparation for cyber-crime helps ensure the best possible outcome. Having roles and responsibilities outlined in advance expedites the response coordination, communication, and ultimately, resolution.

Identify Stakeholders — Assemble the team best suited to address any potential compromise to the organization's electronic resources. Besides

« TO TABLE OF CONTENTS

internal technical professionals, this group may include public relations personnel, customer service support, legal department representatives and law enforcement staff. Agencies should also consider pre-identifying and retaining a specialized technology forensics expert for independent expertise in assembling the IRP.

Make a Plan — IRP plans should include detailed scenarios describing plans of action to address potential events. Sample elements might include strategies for detection and triage, containment, analysis and remediation. Your plan should also identify the point at which various internal and external resources should be contacted.

Prepare Notification Templates — Templates for various communications — such as internal and external e-mails, press releases, online announcements, social media posts and other messages — will facilitate timely communication in the event of an incident.

Conduct an Incident Drill — A full-scale incident exercise is the best way to identify gaps in the IRP. Following the exercise, take the necessary steps to fill in any gaps that were noted.

Keep Plans Up to Date — Schedule a plan review on a regular basis to make any necessary adjustments to stakeholder contact information. Make sure any new potential responders are aware of and comfortable with their duties. In the current economic environment, when staff reductions and agency consolidations are commonplace, this step ensures that every element of the plan is covered and carried out as intended.

FORENSICS

The prevalence of cyber-attacks is prompting an increase in regulatory requirements related to protecting data. In the event of a breach, a comprehensive security policy, including computer forensics capabilities, can help protect against audits or lawsuits.

RESOURCES:
The **Forensic Analysis Methodology Chart** (from the Computer Crime & Intellectual Property section of the U.S. Department of Justice) outlines the process of preparing, identifying and analyzing digital forensic information. www.cybercrime.gov/forensics_chart.pdf

Computer Forensics World is an online community of digital forensics professionals, and features key resources and industry best practices. www.computerforensicsworld.com

Computer forensics is an important tool used to determine the exact nature of a breach, its origin and all the potential impacts throughout an organization's IT infrastructure. Forensic software can copy files to another system for inspection, allowing the original infected files to remain intact to keep evidence from being corrupted. Other forensics utilities analyze file data to identify file extensions that were intentionally altered with malicious intent.

Having staff on site with knowledge of best practices in forensics is important. In most instances, however, relying on internal resources to respond when a breach

« TO TABLE OF CONTENTS

occurs may not be enough. Staff responsible for incident response must find out how and why the breach occurred, collect evidence and thoroughly document any policy violations or potentially unlawful activities that are identified, and most organizations just don't have that level of expertise.

Document the Response — Any internal actions taken prior to bringing in external experts need a thorough paper trail to withstand scrutiny of the process after the incident.

Preserve Critical Information — Ensure that the organization has the necessary tools and knowledge to preserve all information potentially related to the suspected security incident. Protecting this information with forensically sound practices will be vital should the matter advance to legal proceedings.

Retain a Forensics Partner — Select a qualified technical forensic expert appropriate for your organization that can be available for quick response. Execute service agreements in advance of any incidents to keep contract discussions from impeding timely incident response. Consider this external expert's role when formulating the IRP plan.

Look for Experience — Ideal consultants should have experience in effectively identifying unauthorized, illegal or malicious activity, and strong knowledge of the latest forensic tools to trace a broad range of internal and external threats.

Retain Credibility — Using an independent external contractor with the necessary credentials in technical forensics also adds credibility to the incident investigation, providing reassurance to those who may be affected.

Prevent Future Incidents — Be prepared to make the necessary security-related investments to protect the organization from the same type of incident in the future.

CHECKLIST — PLANNING FOR THE WORST CASE

- □ Create a thorough incident response plan, detailing roles and responsibilities in the event of a breach.
- □ Conduct an incident drill to identify any gaps in the plan. Update the IRP as necessary.
- □ Schedule regular IRP updates to incorporate changes in staffing and organizational structure.
- □ Consider retaining a qualified technical forensics expert to expedite response to any incidents.
- □ Make sure internal security experts know what to do if a breach takes place, including documenting their actions and preserving evidence.

« TO TABLE OF CONTENTS

For additional copies or to download
this document, please visit:
public-cio.com/security

at&t