2016 CYBERSECURITY PLAYBOOK

Contents

Intro: The State of Cybersecurity 2016

2015 was the year of more. More malware registered. More personal records lost. More money spent on solutions that don't seem to be having much impact.

In 2015...

140 million new malware
variants were registered. That's nearly **380,000** a day. (AV-Test)

169 million personal records
were exposed in major data breaches. (ITRC)

$75 billion was spent
on cybersecurity worldwide. (Gartner)

If there was a bright side to 2015, it was that cybersecurity continued its rise to the forefront as a serious issue and top business priority. But if we're going to transform that growing awareness into action and measurable progress in 2016, it's going to take more than simply advocating for "more."

We need to make sure we're working not just harder but smarter, and that our efforts are actually aligned with our top needs. This playbook is designed to help you determine what those are for your organization, and to develop a winning game plan for getting more secure.

Part 1: Scouting Report — Top 10 Threats

What Threats Should I Be Prepared for in 2016?

The key to any effective game plan is knowing what you're up against. In this section, you'll learn more about ten of the most common threats your company is likely to face.

- Phishing
- Malvertising
- Software vulnerabilities
- SQL injection
- Password attacks
- Ransomware
- Denial of service attacks (DoS/DDos)
- Drive-by downloads
- Man-in-the-middle attacks (MITM)
- Scareware

Phishing

What It Is:

A malicious attempt to acquire sensitive information by mascquerading as a trustworthy source via email, text, pop-up message, etc.

For as complicated and state-of-the-art as the world of cybersecurity seems, the fact is if your company gets hacked, it will most likely be because one of your employees clicks something they shouldn't. Hackers know your employees are the weakest link, and they've gotten incredibly good at creating phishing messages that not only look legitimate, but also appear to come from sources you know and trust. For an example of a phishing attempt in action, see this email that was sent to our CEO.

How To Protect Against It:

In addition to training employees on how to spot the tell-tale signs of phishing emails, another way to prevent many phishing attacks from being successful is for companies to move away from using email as a way to transfer files. That would allow for blanket "don't open attachments" policies instead of asking employees to determine what's safe and what isn't, and there are plenty of alternative file transfer services to consider.

Malvertising

What It Is:

An attack campaign that delivers a payload of malware by disguising itself as an ad.

When thinking about malvertising it's a good idea to remember that online threats aren't confined to sketchy websites. As a recent attack that infected up to 27,000 Yahoo visitors per hour shows, malvertising can appear on legitimate sites and look like any other ad.

How To Protect Against It:

In addition to exercising caution and a general healthy adversion to ads, companies should make sure their users have updated endpoint protection running on their machines.

Ransomware

What It Is:

Malware that encrypts and threatens to destroy, permanently remove access to, or publicly post data unless a victim makes payment.

Ransomware has been a fixture in cybersecurity headlines, becoming an increasingly popular — and incredibly lucrative — way for attackers to monetize their exploits on systems. The FBI estimates that CryptoWall, one of the most notorious examples of ransomware, has cost U.S. businesses and consumers at least $18 million this past year alone.

How To Protect Against It:

Companies should invest in strong endpoint protection (as well as other layers of defense) to block the introduction of ransomware in the first place, but to really play things safe they should invest in secure, reliable backup for their sensitive and critical assets.

Software Vulnerabilities

What It Is:

Flaws, glitches, or weaknesses discovered in software that can lead to security concerns and exploits.

New software vulnerabilities are discovered all the time (just ask the Adobe Flash Player folks), and left unaddressed they can become easy gateways for cyber attacks and infection.

How To Protect Against It:

Consider investing in patch management software and a working framework to make addressing vulnerabilities a standard practice. As much as possible, it's also a good idea to limit and standardize the versions of OS and applications your employees are running. That will make the process of scanning for vulnerabilities and rolling out patches and updates slightly more manageable.

Denial of Service Attack (DoS/DDoS)

What It Is:

An attempt to make an online service unavailable by overwhelming it with traffic, sometimes utilizing entire networks of infected computers known as botnets , making it a distributed denial of service attack (DDoS).

DDoS attacks can be used by hacktivists take down sites for political reasons (see the attack on the Trump Towers website launched by hacker group Anonymous), or simply used by criminals as another method of extortion.

How To Protect Against It:

To protect your company's website you'll need to find ways of blocking or absorbing malicious traffic. Webmasters can talk with their hosting provider and third-party services for help. For more information on DDoS attacks, see DigitalAttackMap.com.

Drive-by Downloads

What It Is:

An attack that installs malware on a user's machine as soon as they visit an infected website.

Unfortunately, not all malware requires much if any user interaction to be deployed. In the case of drive by downloads, users can be infected automatically simply by visiting the wrong site. As with malvertising, the site doesn't have to look suspicious to be infected — criminals are also able to perpetrate drive-by downloads by compromising legitimate, hi-trafficked sites.

How To Protect Against It:

Since infection can easily occur without a user's knowledge, it's important to reduce both the risk and consequences of an attack. For starters, make sure users are keeping their software up-to-date, endpoint protection is installed on their devices, and don't give admin access to their computers.

SQL Injection

What It Is:

A type of security exploit where an attacker inserts structured query language (SQL) code into an input box or entry form for execution.

As an example, an attacker could utlize a user sign-in form to send a request to the database rather than entering in a username or password. If successful, the attack could grant the attacker unauthorized access to the entire database.

How To Protect Against It:

SQL injection attacks are made possible due to vulnerabilities introduced during software development. For guidance on how to avoid these flaws, see OWASP's SQL Injection Prevention Cheat Sheet.

Man-in-the-Middle (MITM) Attack

What It Is:

A technique where an attacker intercepts and relays communication between two parties or systems in order to capture, send, and receive privileged information.

Hackers can leverage man-in-the-middle attacks to get their hands on access credentials, modify transactions, and further compromise systems.

How To Protect Against It:

Defenses against man-in-the-middle attacks generally include various authentication and encryption techniques to ensure secure connections. Companies may also consider investing in a virtual private network (VPN). See this post for more information on man-in-the-middle attack defenses.

Password Attack

What It Is:

Attempt to crack passwords.

Attackers can also try gaining access to your systems a more old-fashioned way — by attempting to guess your passwords. But while the technique may be an old one, the tools hackers now have at their disposal are cutting edge. Using software and brute force attacks, hackers can crack simple passwords in minutes (check how long it would take to crack a password like your own here).

How To Protect Against It:

Encourage your users to use strong passwords is the short answer. Encourage them to use a password manager is the better one.

Scareware

What It Is:

Malicious software that misleads users into believing they've been infected and convinces them to download a fake malware removal tool that acutally does infect them.

Scareware is rogue security software that preys on users' fears by displaying pop-up warnings that may look like legitimate alerts. Once the user follows the instructions and downloads the software, however, their system is now infected.

How To Protect Against It:

A solid defense involves the typical standards, including firewalls and trusted endpoint protection installed, as well as user education.

Part 2: Establishing Your Game Plan

What Should I Set Out to Accomplish First?

In this section, we'll cover some of the basics, including how to assess your needs to make sure you're focusing on the things that matter most.

Step 1: Assess Your Needs

Security is anything but one-size-fits-all. While it's tempting to take pages from other companies' playbooks, the truth is there's no guarantee their approaches will work for you. That's why the first step for anyone looking to improve their organization's security is to perform a diagnostic self-evaluation. If that sounds complicated, don't worry, it's not. In fact, you can surface a lot from answering two deceptively simple questions:

Question: Why do we need better security?

By asking this question, you can begin developing sharper clarity around your organization's underlying motivations and priorities. What is it that you're most worried about? What are the problems and challenges that improved security is intended to solve?

From there, try to understand the specific reasons your organization isn't secure enough already, and develop focused goals around what you want to accomplish to change that.

Deliverable: A clear mission statement for your security initiative.

Question: What are we trying to secure?

Asking this question up front will help you avoid a doomed and inefficient attempt to protect everything from anything. Instead, you can focus on identifying your most critical assets, assessing the current state of coverage for those assets, and determining what gaps (if any) exist that you want to address.

Deliverable: Inventory of critical assets you need to protect.

As a result of answering these two questions, you should be able to start honing in on the kinds of approaches and security solutions that are going to help not just anyone, but you, specifically.

Step 2: Mind the Gaps

Knowing your specific needs is key. So is covering the basics. When assessing your situation you'll want to consider employing as many if not all of the following fundamental layers of security as possible:

Firewall(s)

A good firewall will help you shore up your perimeter by adding a protective layer between your internal network and any potential attackers attempting to gain unauthorized access.

United threat management (UTM)

UTMs will often combine firewall, content filtering, virtual private network capabilities, and intrusion detection technologies into one solution, making them an appealing option, especially for small- and medium-sized companies.

Endpoint protection

With the majority of infections starting on user systems and quickly spreading from there, endpoint protection is one of the most important layers of your defense. Rather than rely on outdated signature-based anti-virus, your best bet is to invest in a solution that identifies malware based on its behavior.

Security Information and Event Management (SIEM)

SIEM can be thought of as providing a bird's-eye view of your organization's security, offering greater visibility into your network and helping you discover unwanted traffic or behavior.

Data backup

No security initiative would be complete without a solid backup and recovery strategy. In addition to simply being good practice, it can be an effective defense against encryption and extortion attacks like ransomware.

Whitelisting

Application whitelisting can help you reduce the opportunity for infection by limiting the applications and files you allow to be executed. The potential downside is introducing limitations that can negatively impact user and business functionality.

Patch management

The moment a software vulnerability is discovered and a patch is released, it's a race to evaluate and deploy it before the vulnerability can be exploited. Finding a solution that can help you automate patch management tasks can be key to staying up to speed.

Security awareness training

Security isn't just a technology issue, it's a people issue. Errant clicks, user error, and social engineering attacks such as phishing are some of the biggest threats you'll have to deal with. Educating and empowering users to make safer choices is vital to creating a more sustainable and successful long-term defense.

Step 3: Get the Help You Need

Depending on your situation, you may find yourself owning security for your organization without that being your sole responsibility or area of expertise. When that's the case it's important to recognize and acknowledge your limitations in terms of time, resources, and know-how.

Security isn't a "one and done" activity – it requires persistent, hands-on management. If you can't give it your undivided attention you would be well-advised to consider leveraging the following options for help:

Hiring a dedicated in-house security professional

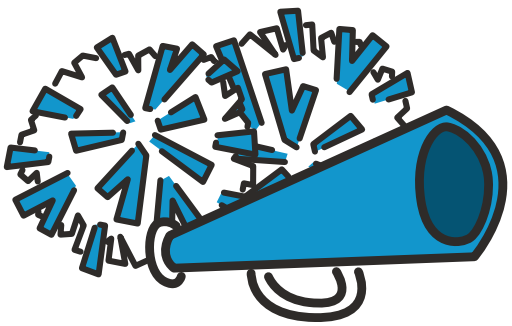
Whether this is a front-line security manager or a full-fledged CISO, the important thing to realize is that if you're going to invest in bringing a security pro on board you also need to invest in setting them up for success. Complicating matters is the fact that we're currently experiencing a global cybersecurity hiring shortage that is driving salaries through the roof.

For tips on making sure your investment doesn't go to waste see our blog post "4 Common Mistakes Companies Make When Hiring for Cybersecurity."

Securing a managed security services provider (MSSP)

For many companies, a more affordable option may be to outsource at least some aspect of their security to an MSSP. Being able to avoid the expenses associated with hiring full-time staff, not to mention purchasing and maintaining costly security solutions, is obviously appealing. That said, outsourcing isn't something you should jump into too quickly. To succeed, it requires a considerable amount of planning, discussion, and building trust.

Keep in mind when it comes to the security of your organization and your customers, the buck ultimately stops with you. If a security incident happens customers won't be looking for an explanation from your MSSP. The blame will fall squarely on you. Before you sign any outsourcing agreements make sure you do your due diligence.



Getting Started with Security

Basic 30-60-90 Day Plan

Month 1: Determine your needs

- ☐ Create an inventory of your "crown jewel" assets (what are you trying to secure?)
- ☐ Take stock of security benchmarks and compliance requirements for your industry
- ☐ Assess your current coverage — do you have the basic layers?
  - Firewall(s)
  - Intrusion prevention system (IPS) and/or united threat management (UTM) that combines firewall, content filtering, virtual private network (VPN), and intrusion detection technologies
  - Endpoint protection (A/V, anti-malware, etc.)
  - Security information and event management (SIEM)
  - Data backup and recovery
  - Whitelisting
  - Patch management
- ☐ Identify your gaps and problem areas
- ☐ Establish your priorities and develop a basic security roadmap

Month 2: Get the help you need and conduct quick wins

- ☐ Determine if you need to hire someone to manage security or if you need to bring in outside help (an MSSP)
- ☐ Assess potential hires, outsourced providers, vendors, and solutions that will help you address your priorities
- ☐ Segment your network components
- ☐ Review user access controls
- ☐ Consider establishing two-factor authentication
- ☐ Secure wireless access points
- ☐ Ensure security policies and procedures are clearly documented with any existing third-party service providers

Month 3: Improve visibility & accountability

- ☐ Focus on gaining more insight into your network and user system activity
- ☐ At the same time, find ways to limit the glut of traffic you need to monitor to reduce noise
- ☐ Establish a reporting dashboard and a regular cadence for reviewing security metrics, both internally and with any outsourced providers
- ☐ Develop a basic employee security awareness program

Part 3: Looking Downfield

What Should I Do to Prep for Long-term Success?

Security is 90% preparation. How successfully your organization reacts to a security incident will largely be determined by the work you put in weeks, months, and years prior. In this section, we'll cover ten important do's and don'ts to ensure you're building a solid foundation of security you can count on when it matters most.

5 Mistakes to Watch Out For

1. Thinking spending more will make you more secure

Gartner estimates security spending reached a record-high $75 billion in 2015, yet we saw just as many data breaches last year as we did the year before. Many companies found out the hard way an expanding budget on its own is more likely to deliver disappointment than added security.

We have a tendency to believe improving security means buying more security, which is why, more often than not, security products gather even more dust than home treadmills. Before you spend another dime in 2016 remember, budget (and technology) is only as good as the people, process, and strategy you have in place to leverage it.

2. Making security purely an IT problem

Data breaches and other security incidents can have ramifications for all aspects of your business, ranging from technical to financial and legal. The issues stretch far beyond the confines of IT, and so should the responsibility for handling and preventing them.

To be truly effective, you need to develop a culture of security that transforms it into a company-wide effort. That starts with a commitment that comes directly from the top (for tips on securing executive buy-in click here). From there, executives need to put pressure on other business units to better manage and take accountability for risk. Finally, there needs to be an investment in training users to behave as your first line of defense (rather than simply the weak link in the chain — see below).

3. Making security purely a user problem

It's well established that the majority of infections are a result of employees clicking the wrong thing. All the more reason to invest in educating and empowering your users to do better.

Unfortunately, by playing the "users are the weak link" card what often happens is we avoid addressing the real weaknesses we have control of (manual processes, vulnerable endpoints, poor password strength-checking), and simply allow users to take the hit for vulnerabilities everyone knows they will trip over.

4. Treating tools and approaches as stand-alone solutions

When evaluating solutions, it's important not to get too focused on individual solutions without taking into account how they can be paired up with additional technology and complementary approaches to your boost overall security posture. Instead, try to focus on how tools interact and enable each other to provide layers of security. Lacking a magical silver bullet (which will never exist), the next-best security is a layered approach.

5. Measuring the wrong things

Once you have a security program in place it's obviously essential to be able to monitor and report on its effectiveness. But how exactly do you plan on tracking that? According to a recent Ponemon survey, nearly 50% of IT pros say the metrics they're tracking don't actually convey the true state of security in their organization.

It's easy to fall into the trap of relying on weak proxies to understand improvements in security rather than focusing on data that correlates to an actual reduction in successful attacks, breach scope, or damage. But when reports present positive progress against the wrong goals they provide a very dangerous sense of false confidence, and reduce the pressure to revisit and improve strategy and practices. It also obscures the remaining risk from management teams who are making judgements based on the data that is served up to them.

5 Tips for Planning Ahead

1. Get leadership buy-in early and often

Your leadership team doesn't have to understand how exactly security works (chances are it will make their heads spin), but they do need to understand why you're doing what you're doing, and be on board with what you're ultimately trying to achieve. The sooner you get them involved in the conversation, the sooner you can a) come to a universal agreement on priorities, goals, and objectives; and b) leverage their help in achieving them.

2. Learn to think of security in business terms

Of course, gaining executive buy-in will be much easier once you understand and accept that leadership's primary concern is running a successful business. If a new security initiative you're proposing can help them do that, fantastic — they will be much more receptive to supporting it if you lead off by explaining how it aligns with primary business goals.

For more advice, see "How to Get Executive Buy-in for Your Security Budget".

3. Invest in employee training

Focusing too much on PEBCAK (Problem Exists Between Chair and Keyboard) can be unproductive (see the previous mistake to watch out for), but the truth is relying solely on technology to solve a human-error-prone problem will only take us so far. Nine times out of ten, malware requires human interaction before it can infect its target. Remove or disrupt that interaction and you can make a huge impact.

Getting users to change their habits and priorities is a tall order. To encourage them, try educating them on how their actions can have a very real real impact on your organization's security — both in a harmful and beneficial sense. Use examples that are personally relevant to them and their day-to-day lives. Focus on positive reinforcement over negative, and don't be discouraged if it takes repetition for the message to sink in.

For more tips for engaging and empowering employees, see our *Realist's Guide to Cybersecurity Awareness*.

4. Establish regular retrospectives and reviews

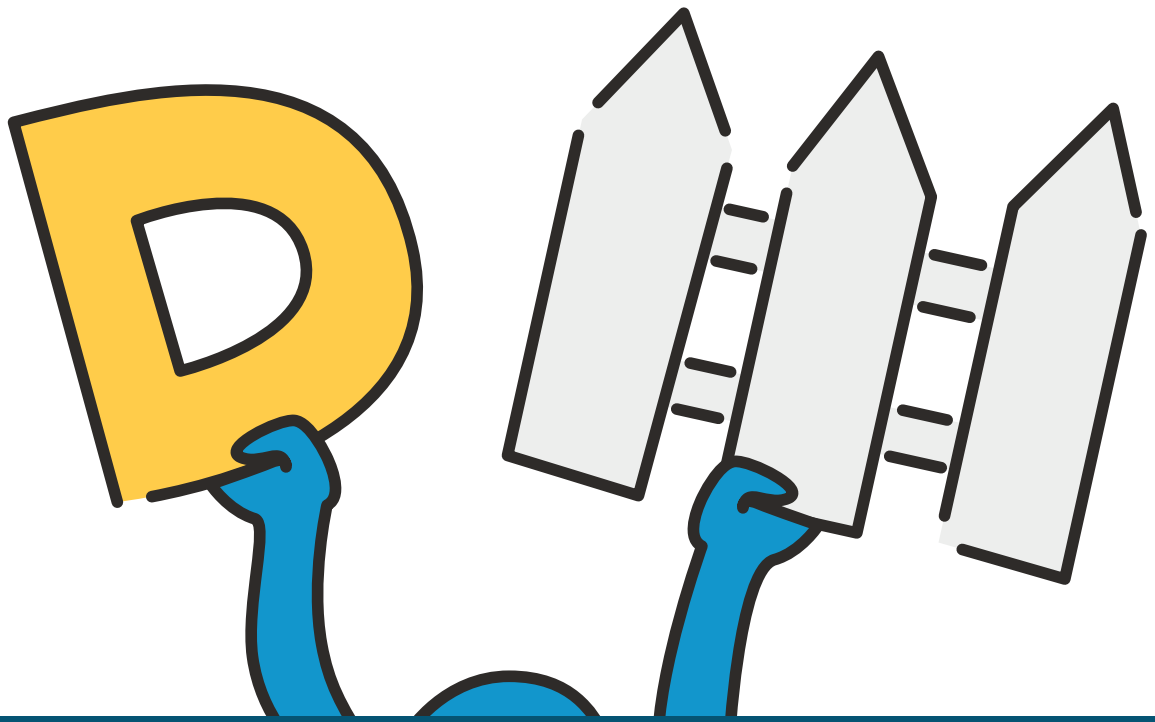
When it comes to improving security you can't just set it and forget it. Without steady iteration it's far too easy for a fresh approach to become the stale status quo, and in the rapidly evolving world of security, stale is seldom secure.

The key is to establish a regular cadence of going back to your plan, reexamining your priorities, reviewing the results against your goals, and discussing what changes or adjustments need to be made to keep everything aligned. Otherwise, you run the risk of discovering too late your budget and efforts haven't actually been flowing to the right needs (what we call the "more money, same problems" pattern).

5. Have a security incident response plan in place

Because incidents can and will happen to you. And when they do, you need to be prepared to act quickly and decisively. The last thing you want is to be caught off guard — the longer a breach or infection goes unaddressed, the more difficult it is to contain, investigate, and address. Damage and cost of remediation escalates quickly.

Working through an imagined worst-case scenario now can help you better determine what tools, people, and processes you'll need to have in place to respond effectively. For a good overview on how to develop your own plan, check out AlienVault's *Insider's Guide to Incident Response*.



Part 4: Overtime

Where can I find more info?

This guide was developed to help you jump-start your security efforts — it's by no means comprehensive. In this section, you'll discover a variety of additional expert resources for diving deeper and determining where to go from here.

Additional Resources

Starting at the Endpoint | The Barkly Blog

Okay, yes, we're tooting our own horn, but our blog really is a great place to grab the latest infosec news and best practices (all in plain English).

The Open Web Application Security Project (OWASP)

A mother lode of information and materials for individuals and organizations looking to make better informed decisions about security risks.

InfoSec Institute

Chock-full of articles, guides, and hands-on tutorials on a variety of security topics.

How-to Questions and Answers

Spiceworks Security Forum

An active community of IT pros at small- to medium-sized businesses asking and answering questions on how to choose the right security product, wrangle your users, and more.

Information Security Stack Exchange

Another free Q&A message board site covering a wide array of security topics, problems, and best practices straight from the trenches.

Security Awareness

SANS Securing the Human

A great collection of free tools and resources to help you develop and maintain an effective awareness program, including planning kits, presentations, and more.

KnowBe4 More free tools and tips for addressing social engineering and transforming employee behavior.

Experts to Follow

Troy Hunt @troyhunt
What to follow Troy for: In-depth analysis of high-profile data breaches (ex: see his breakdowns of the VTech breach) and other real-world examples of hacking in action.

Brian Krebs @briankrebs
What to follow Krebs for: Breaking news and original in-depth coverage of data breaches and cybercrime.

Jessy Irwin @jessysaurusrex
What to follow Jessy for: Inimitable takes on privacy, encryption, and security education with the occasional entertaining rant.

Graham Cluley @gcluley
What to follow Graham for: Quick expert takes on the latest security headlines.

Chris Wysopal @WeldPond
What to follow Chris for: Alerts and reactions to the latest security vulnerabilities plus thoughts on application security, politics, and more.

Katie Moussouris @k8em0
What to follow Katie for: The latest on security research, bounty programs, and vulnerability disclosure.

Lance Spitzner @lspitzner
What to follow Lance for: Tips on improving security awareness with employees and communities at large.

Jeremiah Grossman @jeremiahg
What to follow Jeremiah for: Security industry news and commentary, including reactions to the latest stats and trends.

Violet Blue @violetblue

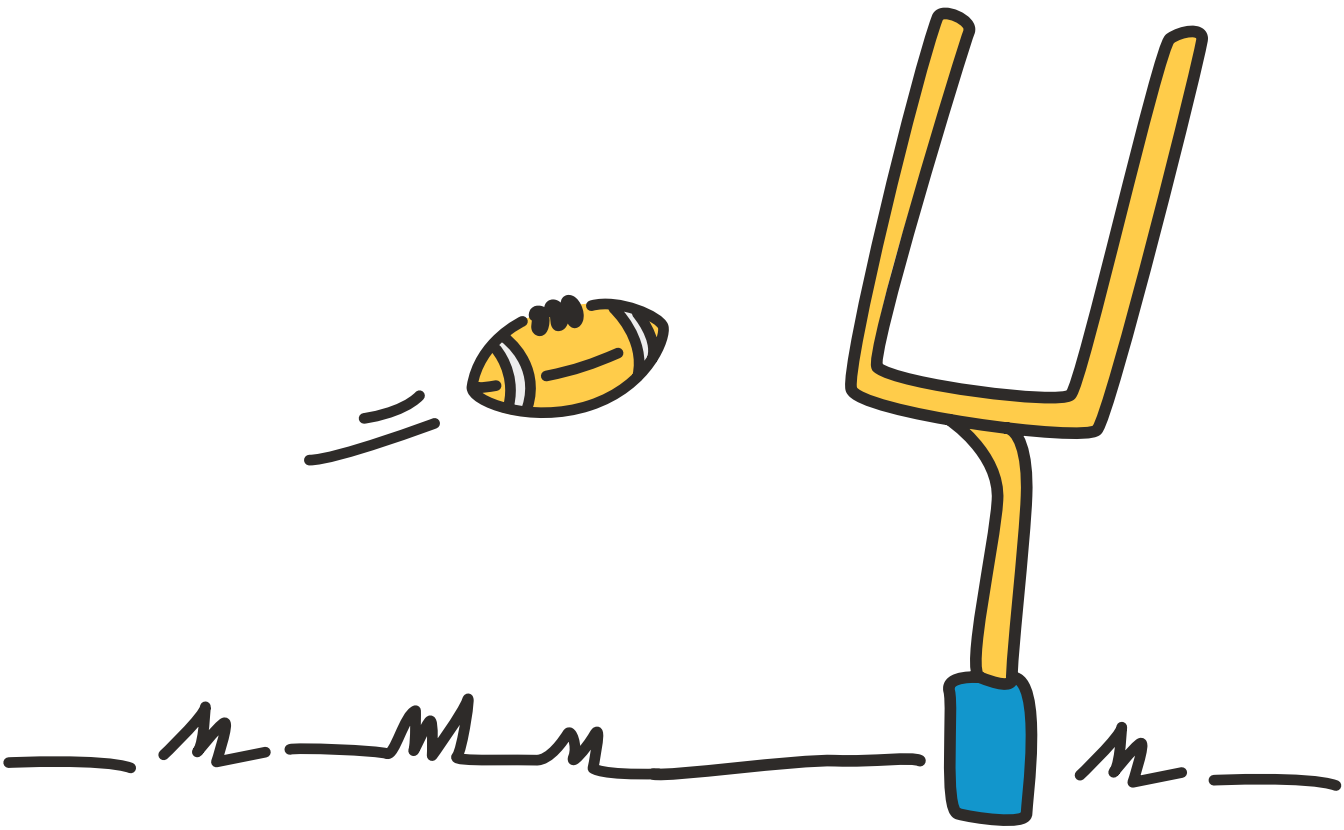
What to follow Violet for: Strong points of view on privacy and security along with practical advice.

Marcus J. Carey @marcusjcarey

What to follow Marcus for: No-nonsense takes on the latest security and privacy debates with helpful how-to here and there.

SecuriTay @SwiftOnSecurity

What to follow SecuriTay for: Biting infosec wit and sarcasm from the mouth of America's sweetheart. Not only are these tweets hilarious, they're also surprisingly effective entries into infosec news and issues.



At Barkly, we believe security shouldn't have to be difficult to use or understand. That's why we're building a simple solution designed to safeguard your company with strong endpoint protection that's fast, affordable, and easy-to-use.

Learn More

Share the 2016 Cybersecurity Playbook on Twitter

Barkly

Stay informed! Subscribe to the Starting at the Endpoint Blog:
blog.barkly.com