OAT Security

Let’s say you’ve never thought about cybersecurity before. Or never thought about it systematically. Sure, you tell employees to use good passwords, and not click suspicious emails. At some point, you put antivirus on a few employee laptops, but you’re not sure which ones. Maybe they’re out of date. Cybersecurity is a bit of a daunting problem, and to be honest, you just don’t have time.

Excellent. Give me 5 minutes right now, and I’ll tell you how to spend about an hour later, and you’ll feel like you’re in much better shape.

I divide security into three categories. Organizational, Analytical, and Technical. (I love oats.) I’ll give you a summary/explanation of each, and then a more thorough to-do list for each that you can go through when you’re done (that’s the hour later).

Organizational security is your employees’ (and their devices and accounts) aggregate resistance to common forms of cyber attack. It emcompasses things like having up to date operating systems on employee computers, and ensuring that employees don’t re-use personal passwords for their work accounts. Because this is the source of the easiest precautions as well as the most common (and most successful) cyber attacks, Organizational security is your highest priority.

Analytical Security consists of thinking ‘antagonistically’ about how an attacker could take advantage of your systems. This can be tricky, but doesn’t really require technical skill, and can help prevent many easily avoidable forms of fraud or cyber attack that basic organizational security might miss. For example, say you have a page on your website that auto-generates a list of potential clients for your employees. If that page is publicly accessible, an attacker could load that page again and again and again until they have your entire client list! Or say you give all your employees full database access - and someone who’s just been fired decides to delete all your tables! Thinking about your security in an analytical sense is essential, especially if you’re handling sensitive or valuable data, or have a complex operational model. It also helps you determine what sort of resources you should be putting into your organizational and technical security.

Technical security is, well, pretty technical. Fortunately, the amount you need to think about technical security scales with the complexity of your technical architecture. That is to say - if you don’t have a lot of technical systems in place, you won’t have too much to worry about here. Basically, every computer you run that’s publicly accessible (server), the publicly accessible applications on those servers, and the network devices that connect them to the internet (routers and firewalls) must be kept updated against recent attacks as well as specifically configured so as to prevent malicious access. If you’re running a server with sensitive information, it’s probably worth hiring a professional to make sure it’s properly configured, or determining whether you can switch to a cloud-based solution. Same goes for any web applications you’ve written yourself. As with the rest of your organization, your technical systems will be safe from most hackers so long as you follow best practice. But for complex technical systems, best practice may involve complex technical rules to correctly sanitize user input, construct IPTables, and manage cryptographic secrets.

So to sum up: Organizational security means covering the nontechnical basics - the system updates and password practices that can prevent the vast majority of attacks against small businesses. Analytical security is your next step: it requires you to think like a hacker, but doesn’t require specific technical knowledge. It puts your organizational security into context, and frames the conversation around how much you should be investing in technical security later on. And technical security might include pieces that should be left to experts, but if you have a good idea of what technical systems you have, and what your analytical ‘threat model’ looks like, you can at least “know what you don’t know” and have very specific technical gaps to fill.

Organizational Security:

1. Accounts:
   1. **Unique accounts:** wherever possible, each employee should have a unique account for all services (ie cloud services, social media)
      1. Action: make a list of accounts that are shared by multiple employees. for each, assign someone to investigate separation/affiliation
      2. Action: Create and associate separate accounts
      3. Alternative: Do NOT have social media accounts with passwords shared amongst all employees. Where possible, associate their accounts with your admin account.
      4. Threats:
         1. What if one employee’s computer is compromised? How difficult would the shared account be to recover?
         2. What if you have a disgruntled employee? How do you remove employee access if an employee is fired or makes threats?
   2. **Unique Passwords:** Ensure employees use passwords different from their personal lives, and ideally different passwords for each account
      1. Action: state this explicitly to employees
      2. Action: give all employees password managers (ie 1password, ~$5/employee)
      3. Threats:
         1. Account compromise usually comes from “credential stuffing” where an attacker uses credentials from another hacked website or successful phishing attempt.
   3. **Two Factor Authentication:** Encourage/Require employees to use multi factor auth for email and other key accounts (apps or keys, NOT texts or calls)
      1. Action: advertise 2FA
      2. Action: Yubi Keys for employees
2. Devices (employee laptops, phones, etc) should have the BLUES. They should be
   1. **Backed up**
      1. Backups should be made of entire devices, or at least work critical files, and stored physically and in the cloud. This can hugely reduce the impact of ransomware attacks.
   2. **Lonely**
      1. They shouldn’t be used as personal computers. Well-meaning employees can accidently download malware from a music or video site.
   3. **Updated:**
      1. Keep OS up to date
         1. action enable auto-updates
      2. Keep other critical software up to date (Word, etc)
         1. action: enable auto-updates
      3. Windows computers should have up-to-date antivirus as well
   4. **Encrypted** - Disk encryption should be enabled on all devices.
   5. **Selfish** - All sharing should be turned ‘off’ on all devices. This includes file sharing, network sharing, screen sharing, etc.
3. Social vulnerabilities
   1. Reduce likelihood of employees clicking malicious links
   2. Don’t allow unauthorized office access

**Analytical Security** - Model Threats x Assets

1. **Assets:** What do you have that’s valuable?
   1. Bank accounts
   2. Client/Donor/employee info
   3. Legit email addresses
   4. Computers
   5. Other valuable data
2. **Threats:** Who would want to disrupt you?
   1. Criminals. Probably always
   2. States? If you’re doing sensitive human rights work
   3. Political actors / hacktivists (potentially)
   4. Personal
      1. Past, present, or future employees?
      2. Competitors
3. Create a **matrix mapping** assets to threats wherever relevant. What would the value of the asset be to the threat? What resources would they be willing to deploy? What are the most likely ways they seek to compromise the asset? What people/devices can access the asset, and how could someone else gain access to it, or those people/devices? For example, consider:
   1. Phishing
   2. Physical Access
   3. Threatening/Hurting Employee
   4. Existing Vulnerability or Misconfiguration (Commodity Exploit)
   5. Previously Unknown Vulnerability (0-Day Exploit)

**Technical Security**

1. **Do you have a website?**
   1. Make sure you have good organizational security around the accounts that handle the website, as well as your domain name.
   2. Provide your website with a certificate so the page can be encrypted. This is important even for non-sensitive information, because it prevents attackers from using your page to deliver malware.
2. **Do you host your website?** (To modify the website, do you modify a database or specific files?)
   1. Make sure the host is up to date and properly configured/secured
   2. If your website is wordpress, you can use wpsec to check your wp plugins
3. **Do you have a web application?** Can Users log into your website?
   1. If so, you should use OWASP as a resource - ensure you are preventing OWASP top-10.
4. **Do you have servers on a local network?** (Are there internal-only resources that can only be accessed from within your office or on a VPN?) They should be properly configured and firewalled. At a minimum, make sure they require password access without default or shared passwords, and that they’re updated/backed up regularly.