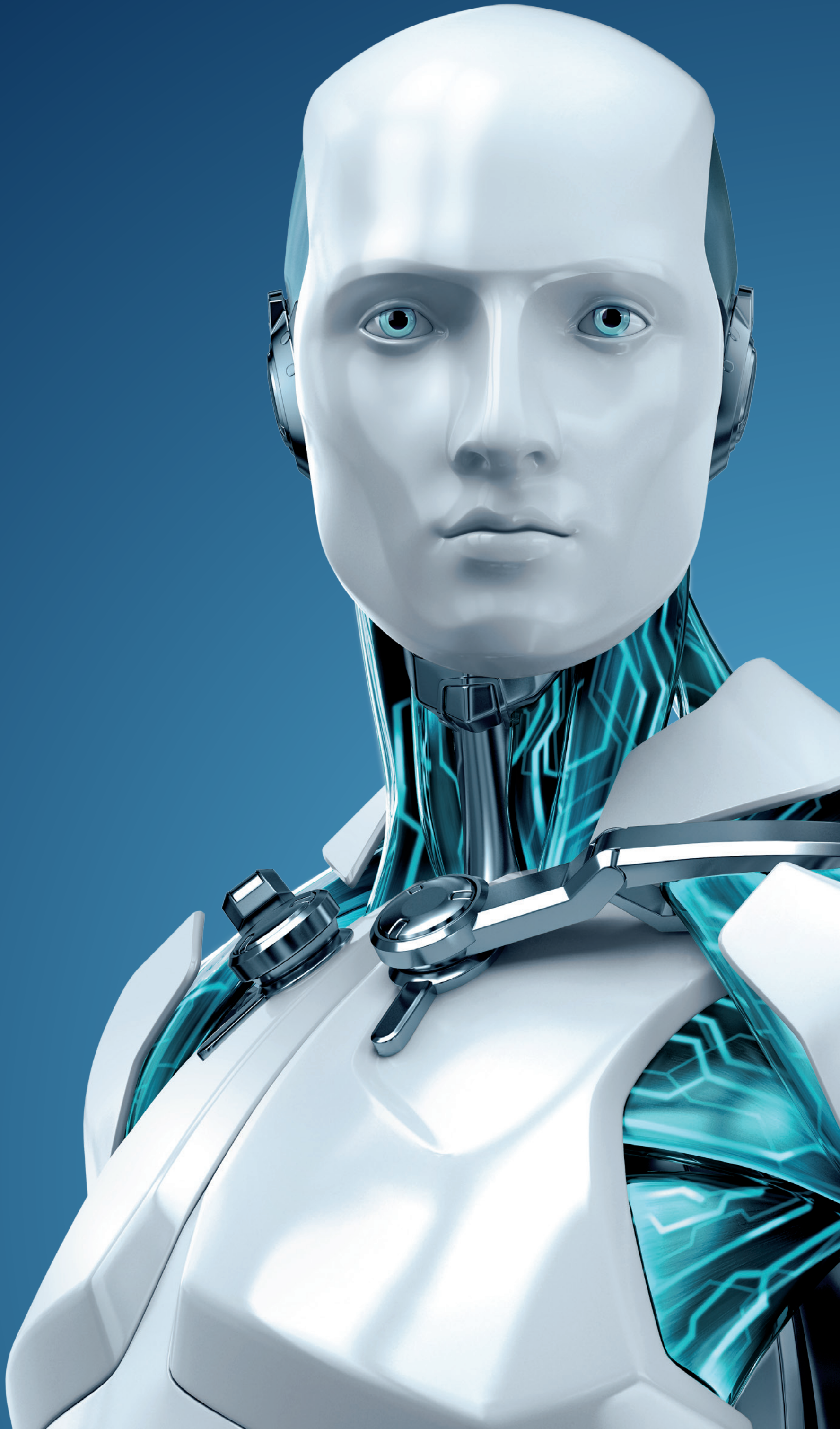
WHITE PAPER

Cyber security road map for businesses



ENJOY SAFER TECHNOLOGY™

CYBER SECURITY ROAD MAP FOR BUSINESSES

By Stephen Cobb, ESET Security Researcher

Criminal hacking is making headlines with depressing frequency these days, so the task of securing your business against cyber criminals can seem daunting, particularly if your business is of modest size, the kind of place that does not have a crack team of cyber security experts on staff. This white paper offers some basic advice on cyber security survival along with links to free resources that can be useful in your efforts to defend your business. There are also a couple of podcasts about this road map.

Cyber security A to F

You can make the task of getting a handle on cyber security more manageable if you break it down into a series of steps.
The following six-step program can help you get started, or revive previous security efforts:

- **A**ssess your assets, risks, and resources
- **B**uild your policy
- **C**hoose your controls
- **D**eploy the controls
- **E**ducate employees, execs, and vendors
- **F**urther assess, audit, and test

Bear in mind that defending your organization against cyber criminals is not a project, it is a process—one that should be ongoing. Too often we see organizations suffer a data breach because the security measures they put in place a few years ago have not been updated, leaving newer aspects of their digital activities undefended.

A: Assess your assets, risks, and resources

The first step in this process is to take stock. What kinds of data does your organization handle? How valuable are they? What threats exist? What resources do you have to counter those threats?

Catalog assets: digital, physical

If you don't know what you've got, you can't protect it. List out the data that makes your organization tick and the systems that process it. (I assume you already have an inventory system for tracking all company computers, routers, access points, tablets, printers, fax machines, etc.)

Be sure to include the systems receiving data and outputting data as well as those that process and store it. For example, if your company depends on a central database of clients and their orders, it is possible to focus on that as your main digital asset, and feel fairly secure because it resides on a well-protected server in a locked room. But connections in and out of that database may come from a wide range of endpoints that exist beyond your physical control. Some of your most valuable data may be highlights and summaries emailed to executives and sitting in their in-boxes. You need to catalog and protect those endpoints.

Determine risk

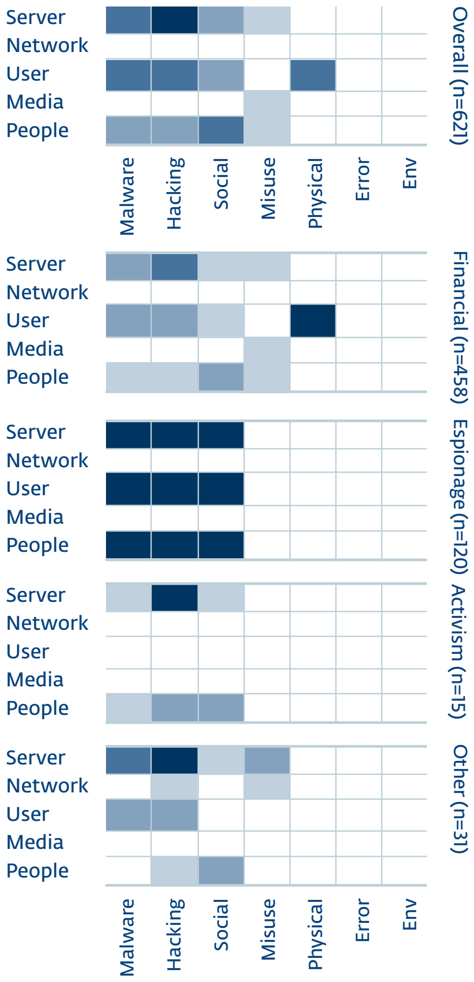
You need to answer this question: What are the main threats to your data and systems? Try stating these in terms of actors, actions, assets, attributes, and motives. For example, some people who don't like your construction company's use of imported timber (actors) might attack (action) your website (asset) to prevent you from taking orders (attribute) to make a point (motive).

This type of breakdown of threats is used in the annual *Verizon Data Breach Investigation Report*, a document worth reading at this stage because it provides a solid background to internal discussions about risks, one that is based on recent real-world attacks.

The report uses something called VERIS—as in Vocabulary for Event Recording and Incident Sharing—to provide a standardized way of describing the bad things that happen to data and systems in terms of: "who did what to what (or whom) with what result."

On the right is a chart from that report, which maps the 621 incidents analyzed by Verizon in 2012, based on actions and assets, broken down by actor motive (darker color means more activity). The action categories are: Malware, Hacking, Social engineering, Misuse, Physical, Error, and Environmental. The motives are Financial, Espionage, Activism, and Other. These are handy schemas to use when performing your review of the risks faced by your organization. The assets are a good way of looking at the focus of the attack.

For help in how to structure your assessment of risk, there is a handy nontechnical Cyber Security Risk Management Guide from the New York State Office of Cyber Security.



Darker color means more activity Dark ● ● ● ● ● ● ● ● ● ● Light

Figure 1: Note that your organization may not fit this "average" profile of activity. Furthermore, this profile is based on incident data that Verizon and its partners analyzed, not the totality of all malicious activity occurring last year.

After cataloging all the digital assets that you need to protect and reviewing the threats ranged against them, you can feel overwhelmed. Now take heart and list out the resources you may be able to tap as you swing into action. This can include current employees with cyber security skills, outside consultants recommended by friends, partners, and trusted vendors. You may be able to get help from trade associations, local business groups, even the federal government. See the resources at the end of this article for some suggestions.

B: Build your policy

The only sustainable approach to cyber security begins with, and depends on, good policy (I think it is fair to say that's the consensus opinion of information security processionals, myself included). Ideally, policy begins with C-level buy-in and flows naturally from there. Your organization needs a high-level commitment to protecting the privacy and security of all data handled by the organization. For example:

> We declare that it is the official policy of Acme Enterprises that information, in all its forms, written, spoken, recorded electronically or printed, will be protected from accidental or intentional unauthorized modification, or destruction throughout its life cycle.

From this flow policies on specifics. For example:

> Customer information access policy: Access to customer information stored on the company network shall be restricted to those employees who need the information to perform their assigned duties.

You implement this policy through controls, which we will discuss in a moment. First, I want to stress that for many companies, no matter how small, information security is not optional. I'm not just talking about legal requirements to have policy, which exist in areas such as health and financial data, but the need to have policies to close deals. These days it is not unusual for a company to ask potential suppliers to comply with requirements like this:

> Vendor must have a written policy, approved by its management, that addresses information security, states its management commitment to security, and defines the approach to managing information security.

That is actual language seen a few years ago in contract negotiations between a small software developer and a large, well-known retailer. In other words, this company is saying, "You don't get to be one of our approved vendors if you don't have written and defined information security policies."

C: Choose the controls to enforce your policies

Information system security professionals use the term "controls" for those mechanisms by which policies are enforced. For example, if your policy states that only authorized employees can access certain data, a suitable control might be:

- Limit access to specific data to specified individuals by requiring employees to identify and authenticate themselves to the system.

That's a high-level description of the control. You will need to get more specific as you move toward selection of actual controls, for example:

- Require identification and authentication of all employees via unique credentials (e.g. username and password).
- Forbid the sharing of user credentials.
- Log all access to data by unique identifier.
- Periodically review logs and investigate anomalies.

Spelling out the controls will help you identify any new products you may need, bearing in mind that there may be suitable security features available in products you already use. For example, if your policy states that sensitive data shall not be emailed outside the organization in clear text, a suitable control to apply–encrypting of documents–may be accomplished through the document password protection features in products like Microsoft Office and Adobe Acrobat. (Note: I'm not saying that these features are strong enough for very sensitive data, but they do make intercepted documents a lot harder to read than ones that are not encrypted.)

D: Deploy and test controls

Putting controls in place is the deployment phase, but this also includes part of the next phase, education. For example, when you roll out a control like unique user IDs and passwords, you will need to educate users about why this is happening and how it works (in this example, that process should include explaining what constitutes a strong password—in my experience, an alarmingly large percentage of computer users have never had this explained to them). You will also need to test as you deploy, to make sure that the controls are working.

A phased approach to roll out often works better than deploying controls all at once because you can identify problems and find solutions while scale is still limited. Rolling out to more experienced users first is a good way to get initial feedback and improve messaging to be used with the wider population (bearing in mind that some things that experienced users already know may nevertheless need to be explained to the general user population).

When testing a control, you need to make sure that it works technically, but also that it "works" with your work, that is, does not impose too great a burden on employees or processes.

E: Educate employees, execs, vendors, and partners

Security education is too often the neglected step in cyber security. In my opinion, for your cyber security efforts to be as successful as they can be, everyone needs to know and understand:

- What the organization's cyber security policies are
- How to comply with them through proper use of controls
- Why compliance is important
- The consequences of failure to comply

Your goal should be a "security-aware workforce" that is self-policing. In other words, employees are empowered to say "no" to practices that are risky and report them to management (even if the persons engaged in unsafe cyber practices are managers).

In terms of consequences, there is no need to sound overly draconian, but you do need to spell out, calmly but clearly, that a breach of security could be very bad news for the organization and threaten its continued operation, including employment.

Two areas of education you don't want to skimp on are executives, some of whom may feel they are above security rules, and partners, vendors, and clients, who need to know what your security stance is, what you allow, and what you forbid. In fact, any data-sharing relationship should be encompassed in policies, controls, and security awareness education. You don't want the negligence of a partner to expose sensitive customer data that was entrusted to your keeping. Saying "it was not our fault" may not cut it when trying to rebuild trust with customers. There's a saying, "You can know a person by the friends they keep," and some people will judge a company by the organizations with which it shares data.

F: Further assess, audit, and test

Step F on the road map is by no means the end of the line. In fact, it is a reminder that this process continues. Once policies and controls are in place and education is under way, it is time to reassess security, by testing and auditing. You can do some of this in-house but you may also want to engage an outside entity to get an objective perspective on your efforts so far.

Best practice is to assess security on a periodic basis and adjust defenses accordingly. Even when there is no audit scheduled, you will want to stay up to date on emerging threats and adjust your controls accordingly. For example, a few years ago it was unusual to see brute force attacks on small business systems, but today that is happening all the time. The implication? You probably need to pay more attention to the security of your web server than you have been accustomed to doing. How would you know this is a trend? One way is to subscribe to good security websites, like Dark Reading,[1] Search Security,[2] and of course We Live Security.[3]

You should also be alert to changes in your systems and connections to your data. For example, there are potentially security implications from new vendor relationships, new partnerships, and new digital marketing initiatives. The departure of an employee is another event that requires security attention, making sure that access to data and systems is terminated appropriately.

Cyber security checklist

Yes, there is a lot to think about when tackling cyber security for your organization. Here are some high points you don't want to miss:

- Do you really know what data you are handling?
- Do your employees understand their duty to protect the data?
- Have you given them the tools to work with?
- Can you tie all data access to specific people, times, and devices?
- Have you tried restoring systems from backups lately to make sure they work?
- Who's in charge of your website hosting, and how secure is it?
- Are you regularly eliminating unnecessary data?

[1] Dark Reading. http://www.darkreading.com/

[2] Search Security. http://searchsecurity.techtarget.com/

[3] We Live Security. http://www.welivesecurity.com/

- Have you off-loaded security to someone else?
    - Do you have a managed service provider, private cloud provider, or public cloud provider?
    - Be sure you understand the contract
    - Remember, you can't off-load your liability or compliance requirements
    - Ask how security is handled, what assurances are given in your contract
- What data security and privacy protection laws and regulations apply to your organization?
    - HIPAA and/or HITECH (covers health data, of employees, or patients, processed for clients)
    - Gramm-Leach-Bliley (covers financial institutions)
    - COPPA, Children's Online Privacy Protection Act
    - PCI security standards (for credit card data, processing, and retailers)
    - Data breach notification (47 states have laws that require notification of consumers whose data is exposed, and these laws may apply to you if you have customers from those states)

Cyber security resources

These are mainly PDF files, mainly from other websites:

- FCC Cyber Security Planning Guide

  http://transition.fcc.gov/cyber/cyberplanner.pdf

- Critical Controls for Effective Cyber Defense from SANS

  http://www.sans.org/critical-security-controls/cag4-1.pdf

- The website for 20 Critical Security Controls

  http://www.sans.org/critical-security-controls/guidelines.php

- The Verizon 2013 Data Breach Investigation Report

  http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

- Nontechnical Cyber Security Risk Management Guide

  http://www.dhses.ny.gov/ocs/local-government/documents/Risk-Management-Guide-2012.pdf

- An example of online cybersecurity training

  http://www.eset.com/us/download/training/

- The SMB Cyber Security Survival Guide (slides showing threats and road map)

  http://www.welivesecurity.com/wp-content/uploads/2013/02/RSA2013-Cobb-ESET-Briefing.pdf

- 45 CFR 165.306 security standards for HIPAA-covered entities

  http://www.law.cornell.edu/cfr/text/45/164.306

- NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems

  http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

- Resources on the Securing Our eCity website

  http://securingourecity.org/resource

Note: We should point out that this road map is just a starting point for securing your data and systems and by no means a complete guide to the entire process.