Meeting of the minds

A quick-start planning tool: checkup for your cybersecurity team strategy.

Any organization planning to build a solid cybersecurity program needs to cover all the critical areas, and to align between business management and cybersecurity management.

This Quick-Start Guide can help you define (or redefine) your cybersecurity strategic plans. Also be sure to visit a more detailed white paper about this process, along with additional in-depth information about this topic.

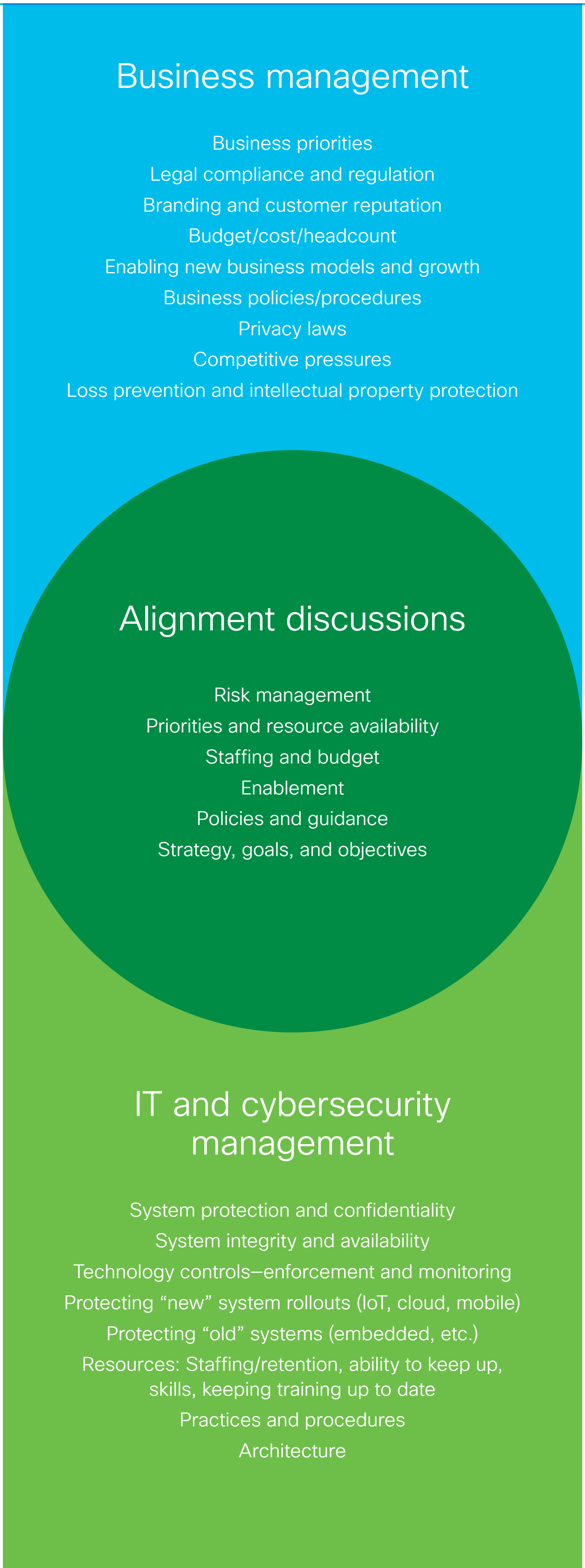
Some questions may not be applicable to your organization. Or you may think of other issues that this guide does not address. Feel free to adapt this list to your needs, to add more questions, or to use it to launch a more in-depth discussion.

© 2018 Cisco and/or its affiliates. All rights reserved.

Meeting of the minds

This diagram shows that, in most organizations, business management appears to be speaking on a different plane from IT and cybersecurity management. But between these two planes is a place in which both groups can–and must–meet to develop a comprehensive cybersecurity strategy.

This list will help both teams work together, so you can achieve a level of protection that benefits the entire organization. Use it as a guide to start the discussion and to develop your own plans.



Business management

Business priorities
Legal compliance and regulation
Branding and customer reputation
Budget/cost/headcount
Enabling new business models and growth
Business policies/procedures
Privacy laws
Competitive pressures
Loss prevention and intellectual property protection

Alignment discussions

Risk management
Priorities and resource availability
Staffing and budget
Enablement
Policies and guidance
Strategy, goals, and objectives

IT and cybersecurity management

System protection and confidentiality
System integrity and availability
Technology controls–enforcement and monitoring
Protecting “new” system rollouts (IoT, cloud, mobile)
Protecting “old” systems (embedded, etc.)
Resources: Staffing/retention, ability to keep up, skills, keeping training up to date
Practices and procedures
Architecture

© 2018 Cisco and/or its affiliates. All rights reserved.

Meeting of the minds

A: What have you got to lose? What are you protecting?

Understand yourself as a target by conducting an assessment.

Identify and catalog your assets:

1. What are the organization’s most and least critical assets? These could include information assets, system assets, customer or patient records, proprietary data, and other assets. List these in descending order of priority.

2. Besides physical assets, what intangible assets could be compromised? These could include your organization’s goodwill, reputation, credit rating, and other assets.

3. What kinds of critical data could be lost to cybercriminals? These could include intellectual property, financial records, patient records, customers’ personal information, credit card numbers, and other data.

4. List any other issues.

© 2018 Cisco and/or its affiliates. All rights reserved.

Meeting of the minds

Evaluate and prioritize your assets:

1. Which losses or damage could cause the most significant financial damage? Think not only of direct and immediate losses, but also long-term such as business slowdowns and loss of brand value.

2. Which losses or damage would most negatively affect competitiveness? Your competitors could take advantage by siphoning off your customers.

3. What would happen if you lose control or access to critical assets? Ransomware attacks could lock your assets until you pay the cybercriminal a ransom to release them.

4. How would a breach affect customers, patients, clients, vendors, donors, and others? Consider how lost business could affect anyone connected with your organization.

5. List any other issues.

© 2018 Cisco and/or its affiliates. All rights reserved.

B: What are your threats and risks?

Knowing what threats you face is an important part of any defense.

Uncover potential threats and risks:

1. Where are the potential security vulnerabilities in the organization? These could be as complex as a full-on network exposure to a cyberattack, or as simple as unsecured company laptops connecting to the Internet. Be as thorough as possible, and consider even the portable devices or files that employees may take home. If you can think of a possible risk, so can a cybercriminal.

2. Which vulnerabilities could cause the greatest losses? Again, think in terms of tangible as well as intangible losses.

3. What priorities should be set for various levels of protection? The more valuable the asset, the higher the priority for protection.

4. What systems and applications should be updated or patched? Often, cyberattacks come through known vulnerabilities that have not been patched or applications that have not been updated.

5. List any other issues.

© 2018 Cisco and/or its affiliates. All rights reserved.

Meeting of the minds

Stay informed about new risks:

1. Does the cybersecurity team have a reliable source of risk intelligence? Without reliable insights and system visibility, your team will be at a significant disadvantage. Your system could be under attack, but your team may not even know it.

2. Does your security team have the proper tools and processes in place so it can respond quickly to an attack? Some attacks last only a few minutes, but they can do significant damage during that time.

3. How's your cybersecurity team uncovering outdated and unpatched systems and applications? The team must be kept updated regarding all the latest information and insights about potential security holes.

4. Does it know how to patch or update systems so all security controls are working? This is where continuing education is valuable. New attack methods require current skills to block them.

5. List any other issues.

© 2018 Cisco and/or its affiliates. All rights reserved.

C: What are your obligations? What are your rules?

Keep informed about laws, regulations, policies, and standards.

Understand and document policies and standards:

1. Which laws and regulations do you need to comply with? Think national-level, local and regional, and industry-specific. You may fall under more rules than you think: Consider the jurisdictions of your customers and partners, as well as your asset list and the types of information you process.

   ____

   ____

2. What's your plan to stay informed on changing regulations? Cybersecurity is predicted to be one of the fastest-growing areas of new regulations.

   ____

   ____

3. What kinds of security policies and standards are already in place? Make a complete list, and determine which assets they're appropriate to protect.

   ____

   ____

4. What kinds of security policies and standards should be created? Think of anything missing. You may check with your industry's professional organizations for ideas.

   ____

   ____

5. Which of them will be most practical to enforce? Some policies and standards may be so complex that staff will ignore or work around them. Think of what will be practical and enforceable.

   ____

   ____

6. What industry regulations must you adhere to, and what's the cost if you don't? Often, the fines for noncompliance can be quite costly.

   ____

   ____

7. List any other issues.

   ____

   ____

   ____

   ____

© 2018 Cisco and/or its affiliates. All rights reserved.

D: What security controls protect you? How do you know they’re working?

Careful selection and management of security controls is vital to an effective defense.

Build, deploy, and enforce policies with processes and controls:

1. What kinds of cybersecurity processes and controls are in place to close security vulnerabilities? Knowing your capabilities should inform your strategy. Make a complete list, and determine which assets they’re appropriate to protect.

2. Are any controls or processes outdated or missing? These could include firewalls, encryption, multifactor authentication, mobile application wrappers, malware detection, biometrics, safeguarded coding, and more. Determine which are most important to purchase and implement.

3. Can you build and deploy your own controls, or must you hire outside expertise? Smaller organizations may find it more cost-efficient to bring in consultants or to purchase off-the-shelf solutions. Larger organizations may find it more efficient to build specialized controls. Security is 24 hours a day, and security controls must operate continuously, even during weekends, holidays, and late into the night.

4. How will you effectively enforce processes? Any process is useless if it’s not implemented and enforced. Make sure that enforcement is part of your plan.

5. Who will monitor and update the controls? Without designated cybersecurity staff to perform this necessary function, it will be ignored. If a security control is out of date or has stopped functioning, it must be detected and addressed.

6. List any other issues.

© 2018 Cisco and/or its affiliates. All rights reserved.

E: Who are you working with? Do they have the right skills? Are you growing team capabilities?

People can be your strongest asset or your weakest link in a security plan.

Hire the right people:

1. Is your organization sufficiently staffed to handle the risks? A cybersecurity team must include more than just an IT person. That’s why it is called a team. They must be able to perform backup, and they should cover for holidays, weekends, and other situations.

   ____

   ____

2. Does your team bring a variety of skills? Make a list and note any gaps. This list may include system architects, security programmers, firewall experts, routing and switching experts, and even those who understand social engineering.

   ____

   ____

3. Do they have a variety of experience levels? You should have a progression plan in place so cybersecurity people are continually moving up the management ladder as they become more experienced. Entry-level people should be taking on routine tasks that aren’t cost-effective for upper management to handle.

   ____

   ____

4. If you don’t have the proper staffing, do you have an outsourcing or hiring plan in place? If you don’t have the right people, then hire them. Note that it’s not imperative to have an entire in-house team, especially if yours is a small organization. In that case, consultants may offer the best solution. Even large organizations may hire consultants for occasional specialized work.

   ____

   ____

5. List any other issues.

   ____

   ____

   ____

   ____

© 2018 Cisco and/or its affiliates. All rights reserved.

Meeting of the minds

Continually expand expertise:

1. Does your team have the necessary skills and certifications for tomorrow's cybersecurity issues? List all certifications and any gaps. Technologies change, and vulnerabilities change with them. Make sure that your team is current with its knowledge and expertise.

2. Are these skills distributed across the team so it can provide 24-hour-a-day and holiday coverage? Are personnel cross-trained? Any good team will have players who can fill in for a variety of positions when necessary.

3. What kinds of certifications should they have? These could include certifications for networking, data center management, routing and switching, or other skills.

4. Should you hire more personnel or consultants who have these certifications? Again, fill the gaps either with in-house staffing or consultants.

5. Does your organization have career development paths for individuals and teams? You should be training and promoting from within so your team has expertise as well as institutional knowledge.

6. Do you use these growth plans to help retain scarce and hard-to-hire cybersecurity professionals? Cybersecurity is a wide-open field, and employees are continually being poached. Your team will remain loyal if they believe that they have advancement opportunities in your organization.

7. List any other issues.

© 2018 Cisco and/or its affiliates. All rights reserved.

Meeting of the minds

Build user awareness:

1. How can all employees be trained to recognize and communicate potential attacks? Typically, employees are the weakest link and can be unwitting victims of social engineering attacks.

   ____

   ____

   ____

2. How often should training occur? These could be comprehensive educational programs once or twice a year, with informal brown-bag lunches each month as refreshers, or some other version.

   ____

   ____

   ____

3. Who will develop and teach the curriculum? Look for two or three people who have broad and deep knowledge of the cybercrime landscape. Trainers can be from inside or outside the organization. But the curriculum should be interesting, educational, and accessible even to non-technical people.

   ____

   ____

   ____

4. List any other issues.

   ____

   ____

   ____

   ____

© 2018 Cisco and/or its affiliates. All rights reserved.

F: What are you doing to keep up to date?

Take resolute action. Don’t make this a one-time exercise. Cybersecurity should be continuous.

Plan and communicate with each other:

1. Do you have a regularly reviewed set of plans to address the attack continuum? Remember that failing to plan is planning to fail. Business and cybersecurity managers should work together on the plan, ensuring it meets all necessities.

2. What is your organization’s plan for what to do before, during, and after an attack? Does everyone know his or her role in the plan? The plan must be communicated and updated. This can be included with your cybersecurity training.

3. Have you rehearsed your plans, and are they revised regularly? Again, this is where the entire organization should participate. Even the lobby receptionist can become a target for a social engineering attack.

4. List any other issues.

Review and evaluate:

1. How often should you review and evaluate all these issues? The best cybersecurity plan will come to nothing if your management team gives it only cursory attention. Protecting your organization and its assets will help to ensure that your operation can continue with minimal disruption and loss.

2. Who will be charged with making sure that it happens? Without assigning a team to follow through, your plan will become shelfware. Be absolutely sure that it is put into action and that it is reviewed on a predictable schedule.

3. List any other issues.

© 2018 Cisco and/or its affiliates. All rights reserved.

Meeting of the minds

Notes

Action items

Follow-ups

© 2018 Cisco and/or its affiliates. All rights reserved.

More resources and help

You're not alone–Cisco is here to help.

For additional copies of this checklist, as well as additional helpful information, visit cisco.com/go/securitytraining.

You'll find training resources, security insights, and a complete white paper with in-depth background about the issues in this guide.

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)