RTAG Working Group on Cybersecurity Policy

Background

In December 2016, Chief Information Security Officer Bob Turner submitted a draft of the proposed Cybersecurity Policy to the RTAG Executive Committee for consideration. Questions posed for RTAG by Bob Turner were:

- Is the policy easy to understand? If not, which areas need clarification?
- Does RTAG agree with the content and intent of the policy?
- Will RTAG 'endorse' the policy to the ITC?

The RTAG Executive Committee discussed the draft proposed policy twice, and determined that a working group should be formed to provide feedback, rather than seeking feedback from the larger RTAG group at this time. The RTAG Executive Group charged the working group with providing a report back to the RTAG Executive Committee and the Office of Cybersecurity detailing feedback on the draft proposed policy from the research community.

Working Group Members

Faculty

Caprice Greenberg	Surgery
Garret Suen	Bacteriology
Jee-seon Kim	Education
Jeremy Morris	Communication Arts

Academic Staff

Rick Konopacki	SMPH
Lee Konrad	Libraries
Ryan Moze	OVCRGE
Carol Pech	Human Subjects IRB
Mark Sweet	RSP
Nicholas Tincher	OVCRGE & RTAG Chair

Feedback on "UW-Madison Cybersecurity Risk Management Policy"

Background Section

1. It would be useful context to provide some statistics or evidence about the current levels and kinds of threats we face and where our systems have not rose to the challenge of protecting our information. Perhaps include various types of threats and threat actors.

Policy Area

1. The document is lacking a clear policy statement around “cybersecurity risk.” The policy says that the process in the document must be followed to manage risk, but this should be the policy that says cybersecurity risk needs to be managed for all UW-Madison data. As written, it’s asking to be inferred rather than directly stated.
2. It is unclear what the scope of “data” or “information” is within the document. This is a policy around managing risk of *all information systems* that *store or process data* used to carry out the missions of the university. That doesn’t clearly articulate external data sets that may be researched, for example. Defined as is, the policy is too broad and vague. IT professionals feel as though they are already following
3. IT professionals feel as though they are already following many/all of the principles but the document doesn’t describe (or refer to a document that describes) how to measure this and confirm they are.
4. The policy should discuss who has jurisdiction over the various parts of the technical infrastructure. For example, who has jurisdiction over the campus network, who has jurisdiction over servers that access the campus network, and who has jurisdiction over the software running on those servers? (This is also pertinent to the “Risk Executive Concept” section).
5. The policy should discuss satisfaction of terms and how an acceptable risk level will be certified. If a contract or federal sponsoring agency provides their conditions of satisfaction, and a researcher believes they are satisfying those conditions but the Office of Cybersecurity does not, which entity prevails? The policy discusses “failure to comply,” but not within a specific timeframe or what happens with systems that were once in compliance and fell out of compliance.
6. There is a need to distinguish between levels of security, data security paradigms (PCI, HIPAA, PHI, etc.)
7. Specific to “Principles” #4, it would be good to have clarification around due process (can monitoring start any time on anyone, or is there a cause that’s needed?). This section, and its implications are not clear.
8. Specific to “Principles” #5a, it would be safest to define this a bit more so that it wouldn’t be abused. What is the definition of “temporary” in terms of threat levels and timeframes?
9. Specific to “Policy” #1, it would be helpful to describe (or refer to a document that describes) exactly how risk is determined. The remainder of the process would seem straightforward with a strong definition of how risk is determined.

Risk Executive Concept

1. Roles of the risk executive need to be very clear, and should be written into the policy.
2. The policy should discuss how jurisdiction over the various parts of the technical infrastructure is determined. For example, who has jurisdiction over the campus network, who has jurisdiction over servers that access the campus network, and who has jurisdiction over the software running on those servers? This may be three different risk executives. What is the best way to work through inheritance, and chains of risk executives?

3. The document should describe the role of the Office of Cybersecurity with respect to Risk Executives. What sort of training and compliance is necessary to be a risk executive, and how will the Office of Cybersecurity facilitate and validate this?
4. It should be understood that Data Use Agreements are with the university, not individuals. What will be the expectation of risk executives who are speaking for/on behalf of the university?

Process

1. The presented document assumes an outside attack or outside threat actor and doesn't speak to internal threats, or threats from groups who have some sort of access to the campus network.
2. The document doesn't speak to how to onboard data and systems already within our ecosystem in order to be compliant with the policy – only that the process will be phased in, with high risk systems first. How are "high/moderate/low risk systems" determined and by whom? Is there a target timeframe for campus-wide compliance with the policy? Once this is determined, the process seems straightforward.
3. There is a sense that the document is trying to do too many things in one fell swoop. Perhaps think about breaking out pieces into separate documents. This doesn't seem to be something that can be operationalized as written. Some policies, particularly where HIPAA compliance is involved, can be referenced.

Resources

1. Recognizing that cybersecurity is a changing landscape, how will the document be updated and future proofed?
2. Recognition that Office of Cybersecurity does not have enough staff to adequately meet the aspirations of this policy. The level of resources within Cybersecurity currently cannot not match the needs and demands of the campus even without enacting this policy. What is the best way to adequately make resources available? What additional resources are needed?
3. Approach currently seems to be one-off for each information system. Are there ways to create some economies of scale with like systems?