



Protecting 'What Matters'

June 2011

Who am I?



Douglas Ferguson – Co-founder & Principal @ Aurora

Barclays Bank – London, UK

- Global Head of
 - Security Controls Assessment
 - Penetration Testing
 - Firewalls
- Account Executive
 - Wireless Security
 - Network Segmentation
 - Denial of Service

Internet Security Systems (ISS)

- X-Force R&D
- X-Force Consulting

Royal Canadian Mounted Police

- WAN Security

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent

Check-ups



What is a check-up?

Why do you go?

- Prove you are healthy
- Find problems and advise treatments

Is this really all?

Property of Aurora Information Security & Risk
This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information.
No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent

What is a check-up? Is it anything other than an objective statement of your health reality?

Why do you go?

1. Prove you are fit
2. Find a problem and get treatment advise

How else do you *know* if you have EARLY cancer, heart disease, hypertension, diabetes, etc.?

Is this really all?

No. Most simply, you're trying to protect 'what matters' most. Your existence.

Deeper, Isn't the real reason because there are others that depend on you? You need to be around, and useful, for others.

You are RESPONSIBLE for remaining alive and healthy. You are ACCOUNTABLE for your actions, behaviors.

So, having a 'check-up' is really due diligence. If you don't do it, you're hurting others.

The 😊 reality



I see 'experts' & best-of-breed technology

I see lots of spend & activity

I see lots of reports, 'successes', promotions, etc.

I see lots of good intent. Winning rocks!

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent

I see experts & best-of-breed technology – I see deployments of network scanners, application pen tests, firewalls, intrusion detection and prevention, malware detection and blocking, encryption, anti-virus, audit after audit after audit, PCI compliance, etc ... you get the picture.

I see lots of spend & activity – People are busy, no question there. But is busy-ness proof of progress?

I see lots of reports, 'successes', promotions, etc. – monthly & quarterly reporting, vulnerability fixing, system patching, blocked virii, etc. successful projects, people get promoted for doing 'great work'. Cool.

How could all this work, spend not get results that make a real difference? It's difficult to believe.

The ☹️ reality



Most orgs can be critically impacted – easily

Worse, many don't know it

Worst, many believe they are safe

Wait, what? How can this be?

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent.

Reality - The pandemic

I've been checking business protection health for years – and the news isn't good – but it's consistent!

Most businesses can be critically impacted by credible threats – *I can prove it*

Worse, many don't know it

Worst, many believe they are healthy

Everyone is impacted: businesses, organizations, governments, etc. off all sizes, industries and locations.

Proof

-Since 2000 I've 'engaged' 100's of companies in dozens of countries – including many of the Global Fortune 1000 across a wide breadth of industries, including: financial services, insurance, pharmaceuticals, retail, transportation, government, academia, healthcare, manufacturing and technology
-I've conducted pen tests, red team exercises, reviewed command & control, strategy, reporting, interviewed leadership

-I've personally proven

- The ability to shut down electricity for an entire country
- The ability to shut down transaction processing for an entire bank
- The ability to 'own' all ATM details for an entire country (plus, shut it down if desired)
- The ability for a bank to fail to adequately respond to a worm and lose the business for 4 full days
- The ability to shut down a data centre without entering the building
- Countless times I've gained unrestricted physical access to offices & network with access to *everything*

The unfortunate



'Innocent' self-deception

- It's an IT problem
- We're not important enough to target
- I don't have enough budget
- Leadership doesn't 'get it'
- Our security is fine – I can 'prove' it
- We haven't been hacked yet!

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent

The industry isn't helping, it's confused. The wrong message is everywhere.

- Self-deception – The action or practice of allowing oneself to believe that a false or unvalidated feeling, idea, or situation is true
- Confirmation bias: Gravitating towards sources of information that validate what you want to believe, and discrediting countering points
- The more you know, the more you know you don't know

It's an IT problem

- Several flaws with this.
1. News is sensational
 2. Tip of iceberg – doesn't reflect what's hidden under the surface
 3. Most technical hacks are on a foundation of personnel, physical, or information hacks
 4. IT's job is to produce secured IT assets in compliance with Security's requirements. Security's job is to ASSURE this is the case.

Security's job is 3 fold:

1. To define the 'law' as agreed by executive leadership. (Policies, standards)
2. To inform business of these laws, their value, and help business achieve lawful behavior
3. To assure the laws are being followed, and apply incentives for those that do, or punishment for those that don't

The actual 'security' is done by the business. Thus, IT builds and maintains secure systems, applications, storage of data, etc. and Security assures this is done adequately.

Dive a car analogy:

1. Gov't defines the speed limits. (LAW)
2. Police use radar, lasers, etc. to enforce this limit. (ASSURE)
3. But who drives the car? You do. Not the gov't or police.
4. In the same way security doesn't secure the business – it makes and enforces the laws.

We're not a target, we don't do anything 'interesting'

Well, yes you are a target. If you have money, customers, or competition you are a target. It's not what you 'sell' that the criminals want – it's your money, revenue potential, secrets (to sell), or just your systems and Internet pipe for a botnet. Most crime you will never know about. Criminals don't want their money source to dry up.

If a criminal wants \$50M they don't care where they get it from – easiest & safest route is the preference – who are the easiest and safest? Those who don't see it coming

Don't have enough budget?

1. Protection is a function of the executive leaderships business plan. You only need to do what they want done.
2. Your job is to articulate risk in a way that they understand.
3. This is a HUGE language gap today.
4. In summary, you should only protect to stated risk threshold specified by leadership
5. Anything more is overspend
6. Anything less is too much risk.
7. You just need to show that your plan, and actions, meet their expectation. That's it.

Leadership often 'doesn't get it'.

But why? Are they fools? Too busy? No, they have time for 'what matters'. It's your job to articulate it clearly in terms leadership understand. Show them 'what matters' and they will listen.

Our security program is fine – I can prove it.

1. Many security leaders point to management reports, pen tests, vulnerability scans, malware blocking, intrusion attempts and blocks, audit reports, compliance (PCI, ISO 27001), etc. as proof the program is working.
2. What does this really prove?
3. What is the goal?
4. What is expected by leadership?
5. That is the only actual proof.
6. If leadership expects that customer data cannot be stolen by hackers, have you validated that?
7. Does PCI compliance secure your payment system and data?
8. No. What's your expectation from PCI compliance?
9. What does your leadership expect?
10. How do you prove it?

We haven't been hacked yet!

1. How do you know? Over 90% of crime is covert – silent. Long gone are the days of EGO Hacking (of course, this is being fogged again by Hactivists).
2. How do you know you don't have cancer right now?
3. You just feel happy and fit?
4. Or, have you recently had a deep specialist inspection?
5. How important it is to you will determine how much you're willing to effort to know your current reality.

Why?



Misaligned or missing protection strategy

Inadequate protection 'checks & balances'

Consider:

Maginot Line, Whack-a-mole, NY Rangers 😊

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent.

Strategy

1. What are you trying to protect?
2. Is this the right stuff to protect?
3. What are the likely threats? And why?
4. What's motivating them? Money? Politic? 'Big Business'? Religion? Environment?
5. What are their goals? How can they achieve those goals?
6. What are the likely targets? And why?
7. What's your plan to protect these?
8. How do you prove progress?
9. How do you know you have the 'right' plan?
10. Do you have the right Roles? People? Processes? Technology? Partners? Measurement?

Can you win a tough battle without a strategy?

Can you gain support of leadership without a strategy?

Checks & balances

What should you protect? What's threatening it? How can it be impacted?

What does leadership EXPECT of the security program?

How are you PROVING you are protecting what they expect?

The ONLY way to prove you are protecting the business is to actually challenge the business from the threat perspective.

Great examples

The Maginot Line. Maginot Line has come to mean a strategy or object that people put hope into but fails miserably.

Whack-a-mole (firefighting). An other symptom of missing strategy is firefighting.

Opportunities



Don't panic – nobody is pointing fingers

This is an opportunity – be an opportunist

This can really advance your career & help your company **BIG TIME**

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent.

How do I solve this?



1. Ensure the 'right' protection strategy
2. Gain leadership support
3. Implement proficiently
4. Assure effectiveness & tune

Property of Aurora Information Security & Risk
This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information.
No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent

Strategy

Has a war ever been won without a good strategy? Has a Superbowl ever been one without a good strategy? Lots of examples of lost wars and games with bad strategy. Heck, even dominate numbers or superstars don't matter if your strategy is flawed.

Support

Only leadership can decide what risk is acceptable (they are paying and accountable), your job is to show them the risks, and let them decide.

Plan

Now that it's agreed what you must protect, you need to do it. Expectation is set, you're on the line for that.

Verify

Just like going to the doctor, your business needs regular check-ups, diagnose 'issues', and treat them. Dependant on the size and value of your assets

Works at ALL levels

This works at all layers of the protection plan (IT example)

- Head of security
 - Head of IT security
 - Head of secure engineering
 - Head of secure platforms
 - Head of secure Windows

'Right' strategy



1. Goals – *What matters?*
2. Command & control – *Roles & accountability*
3. Business integration – *Solve business problems*
4. Risk management – *Protect to expectation*
5. Control framework – *Proactive vs. reactive*
6. Assurance – *KPI's, checks & balances*

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent

Goals

1. CEO & Board – ensure max profit, continued competitive operation of business and maximal valuation
2. Security Officers – ensure security 'incident' doesn't impact CEO's goals

Lots of different kinds of incidents:

Could people die? Building burn down? Identify theft, loss of customer data, lost laptop, failed merger or acquisition, etc.

But the business impact is all about money – not incidents, vulnerabilities, etc. per se. it's the realization of an impact that 'matters'.

Impact business P&L

- Reputation/Embarrassment
- Depressed share price
- Loss of income
- Legal/regulatory consequences
- Unforeseen costs
- Loss of management control
- Loss of competitiveness

Command & Control

The 'right' protection hierarchy must be in place. There are 2 significant side effects if this is not respected:

1. Significant conflicts of interest (example: IT in charge of assuring IT security)
2. Protection unaccountability resulting in unmanaged gaps.

Business Integration

Security exists for the business, not ourselves

If it obstructs, it fails

If it doesn't protect to expectation, it fails

If it doesn't deliver value, it fails

Protection success is a simple cost/benefit proposition

Risk Management

1. Must understand business assets and their value to the business
2. Must understand how to mitigate risk by application of security controls
3. Must understand leaderships risk appetite
4. Explain cost to protect to various risk appetites
5. Gain leadership risk appetite agreement
6. Measure mitigated risk – too much protection is wasted, too little is increased risk.

Control Framework

Controls mitigate risk – they are applied to assets to a degree to reduce risk to desired levels.

Assets types:

1. Business Assets
2. Foundational assets: Compliance, Continuity, Information, Personnel, Physical, Technology
3. Proactive Controls
 1. Predictive Controls
 2. Preventive Controls
4. Reactive Controls
 1. Detective Controls
 2. Responsive Controls

Assurance

How do you know the strategy is right?

How do you know command is in control?

How do you know business assets are protected to expectation?

How do you know a control is effective?

How do you know a control is necessary?

Executive buy-in



Protection is a simple value proposition

1. Enumerate & value business risks
2. Justify costs for asset/level of protection
3. Executives agree/fund protection level
4. Prove return-on-investment

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent

This is critical as the business looks to you for a very important capability – protection of the business. Their careers depend on you.

Enumerate & value business risks

Articulate risk in terms leadership understand and care about – money.

What's the cost of an impact? Immediate loss of revenue? From brand hit? From penalties? From fixing the problem?

- Loss of intellectual property? Product line invalidated?
- What is the impact if the CEO leaves for a competitor?
- What is the impact if the business can not operate for 24 hours?
- What is the impact if IP is leaked to a competitor?
- What is the impact if financial results are leaked early?
- What is the impact if a M&A is leaked to the public during negotiation?
- What is the impact if OC leaches 10% of revenue annually?
- What is the impact if power fails to the primary datacenter for 24 hours?
- What is the impact if phones don't work in HQ for 24 hours?
- What is the impact if email is compromised?
- What is the impact if a mobile phone is lost at an airport?
- What is the impact if an executive laptop is stolen?
- What is the impact if an employee accidentally unleashes a worm on the internal network?

Justify costs for asset/level of protection

- Budget request: CapEx, OpEx costs – over time

Executives agree/fund protection level

- This step is critical – this establishes liability in case of incident
- Also establishes clear expectation on what will be protected, when, and how much it will cost

Prove return-on-investment

- This has several advantages
- Proves your progress toward your objectives and goals
- Proves you are protecting what you should be protecting (checks & balances)
- Proves the degree of protection you are providing
 - Too much is wasted spend
 - Too little is increased risk (your liability)

Implement & operate



Roles – Invest in the ‘right’ people

Process – Necessary & LEAN

Technology – Is a tool, not a solution

Partners – Choose wisely, they are ‘tools’

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent.

People

Your greatest asset is people. People make or break the success of all roles – each role is critical to the success of the protection system – thus, everybody is critical. Ensure the right blend of skills, experience, motivation and attitude for each role. You are not putting a ‘bum in a seat’.

Process

Eliminate waste, bureaucracy. Prove the value of ALL requirements & processes to the primary objective – eliminate if it obstructs rather than supports. All processes must be LEAN.

Technology

Technology isn’t a control, itself, it’s a tool helpful in implementing a control. Any tool can be misused. Security tools can easily mis-inform, worse, they can provide a false sense of security.

Partners

Insource, outsource, supplement, etc. Every task has it’s risk. Bringing in the right skills, as necessary, is fine – as long as it’s managed properly. Otherwise, you introduce more bad than good.

Trust, but verify



Counters self-deception

- Does reporting reflect reality?
- Is protection to expectation?
- Prove return-on-investment
- Advise improvements to strategy & tactics

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent.

Nice side effects



Prove a job well done = bonus + promotion

- Self-determinism
- Solve your bosses problems
- Prove the business value
- Prove return on investment

Property of Aurora Information Security & Risk

This document & the information contained herein is the property of Aurora Information Security & Risk LLC and contains strictly private, confidential and potentially legally privileged information. No unauthorized access, viewing, disclosure, duplication &/or dissemination of this information in whole or in part is permitted without Aurora Information Security & Risk LLC legal consent

-you'll find that this goes along way in your business career – you'll always be ahead of your peers when you have the right plan, and can prove it

-otherwise, all it takes is a single critical challenge from a senior leader and your house of cards collapses

-to be a top security officer you don't have to be a top security expert.

-you need to have a strategy – and that is a business proposition

-if done correctly, the liability is off your shoulders and on senior leadership, where it should be

-so, anybody can be a successful, vigilant security officer

-and a vigilant leader, with justification for actions and proven ROI will be among the top of the list for promotion