Measuring the Return on IT Security Investments

Matthew Rosenquist
Intel Information Security Strategist
Presentation based on Dec '07 White Paper

Public

IT@Intel

With respect to the MiniMetricon audience, this is the condensed presentation. Full details are available in the whitepaper and blog discussions at communities.intel.com

Legal Notices

This presentation is for informational purposes only. INTEL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino logo, Core Inside, FlashFile, i960, InstantIP, Intel, Intel logo, Intel386, Intel486, Intel740, IntelDX2, IntelDX4, IntelSX2, Intel Core, Intel Inside, Intel Inside logo, Intel. Leap ahead., Intel. Leap ahead. logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, IPLink, Itanium, Itanium Inside, MCS, MMX, Oplus, OverDrive, PDCharm, Pentium, Pentium Inside, skoool, Sound Mark, The Journey Inside, VTune, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Last Updated: Aug 28, 2006

Business Challenge

Security programs strive to prevent undesirable events and/or lessening their effects

Determining value is problematic, requiring measurement of events that did not happen and losses avoided

To date, the industry has lacked accurate, quantitative methods for determining ROSI

Business Challenge (cont.)

- Most organizations rely on qualitative methods, which are vague at best
- Difficultly to prioritize and compare against other capital investments
- Lacks detailed financial figures that business decision makers demand
- Determining value is critical for investment in an efficient security strategy

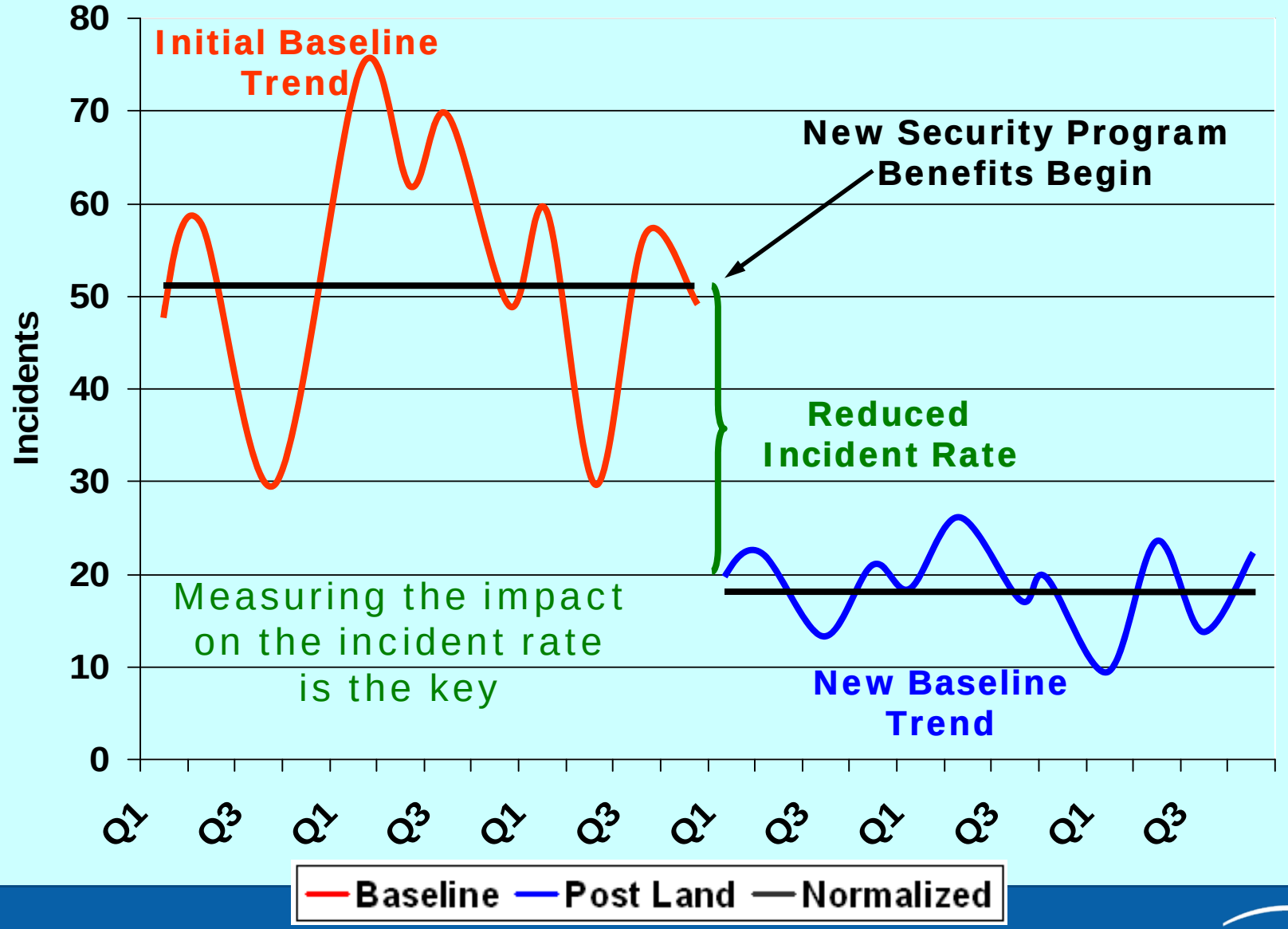
Solution

- Method for estimating the number of future security incidents
- Incident prediction accuracy can be validated!
- Leverages historical data in similar environments to anticipate impacts in the target community
- Avoids arbitrary risk/vulnerability/exposure analysis
- Results showed a highly acceptable degree of accuracy, exceeding all other plausible methods

Solution (cont.)

- Applicable to ‘reduce the occurrence’ type of controls and not applicable for ‘reduce the effects’ security programs
- Requires significant incident trend data prior to and post implementation of the security program
- Requires estimated average value of losses for events

Calculating the Rate of Occurrence



Pre / Post Value Determination

Predict value (pre-deployment to target environment)

- Identify limited control and treatment groups which are similar to the target group
- Measure the improved security of the treatment group against the control group baseline
- Apply the delta to target group and extrapolate to predict the value

Validate prediction/Measure Value (post-deployment to target environment)

1. Measure the actual improved security to the target group
2. Calculate value and compare to prediction

Calculating the Annual Loss Expectancy

- Calculated the Single Loss Expectancy (SLE) for different environments
  - Determine the relationship between incidents and loss
  - Derive a single loss expectancy based on business management and finance estimations and downtime costs
- The impact analysis determined the Annual Rate of Occurrence (ARO)
- Annual Loss Expectancy (ALE) could then be calculated via ALE = SLE x ARO

Case Study

Objective: demonstrate the value to management of 3 proposed security initiatives

Business Environment:

- Intel maintains one of the most complex manufacturing environments which is highly adverse to disruption
- Our factories and manufacturing sites are not identical; the greatly different environments are reflected in both the number of incidents and their impacts
- Proposed programs represented a significant financial investment as well as downtime for integration
- Programs were complementary and expected to reduce security incidents that cause disruption

Case Study

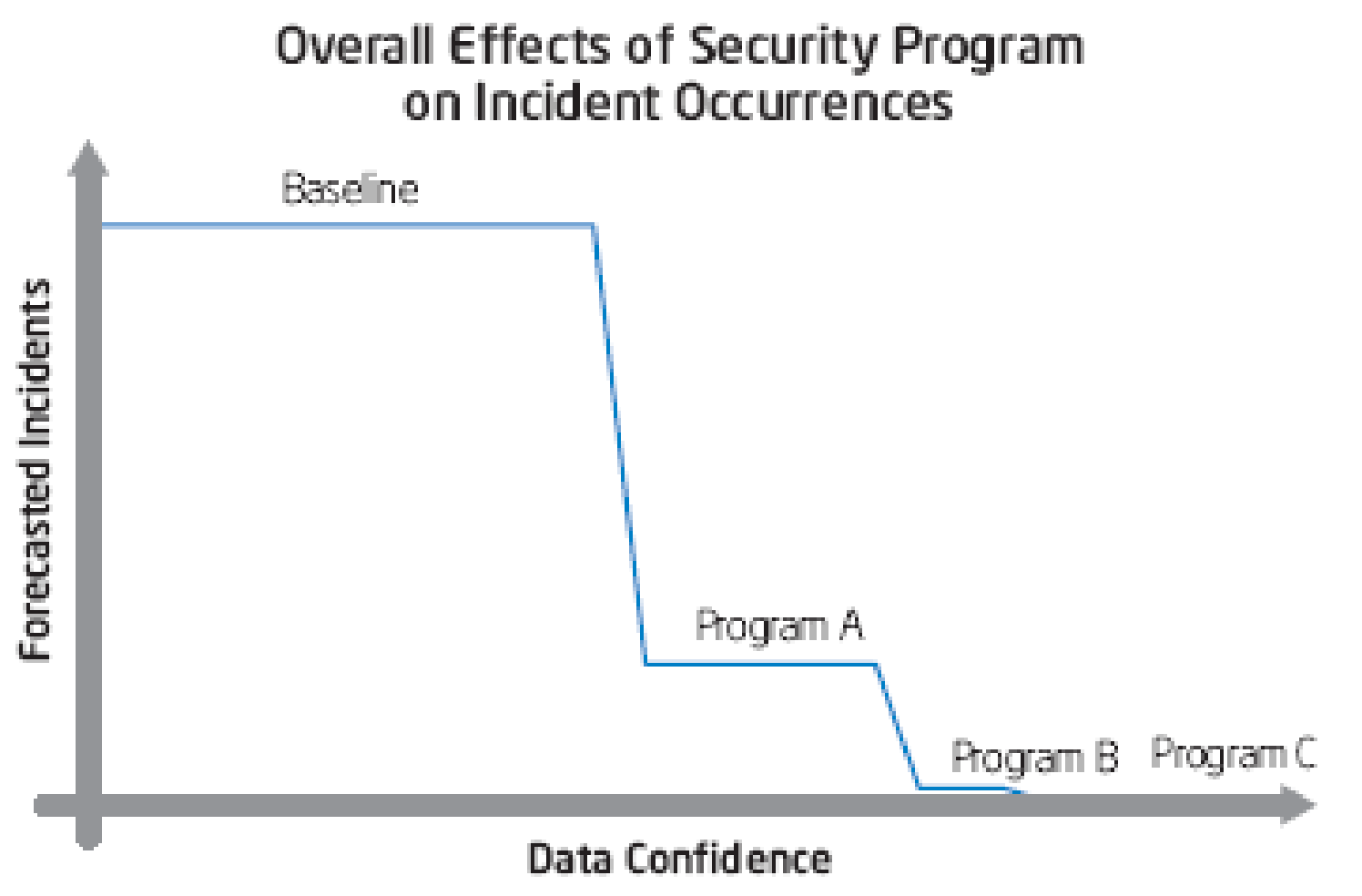
Study Group:

- Incident data (ex. virus and worm events) tracked for two years
- ~18,000 computers over 750 days (equivalent to 13 million computer-days)
- ~20 major locations around the world

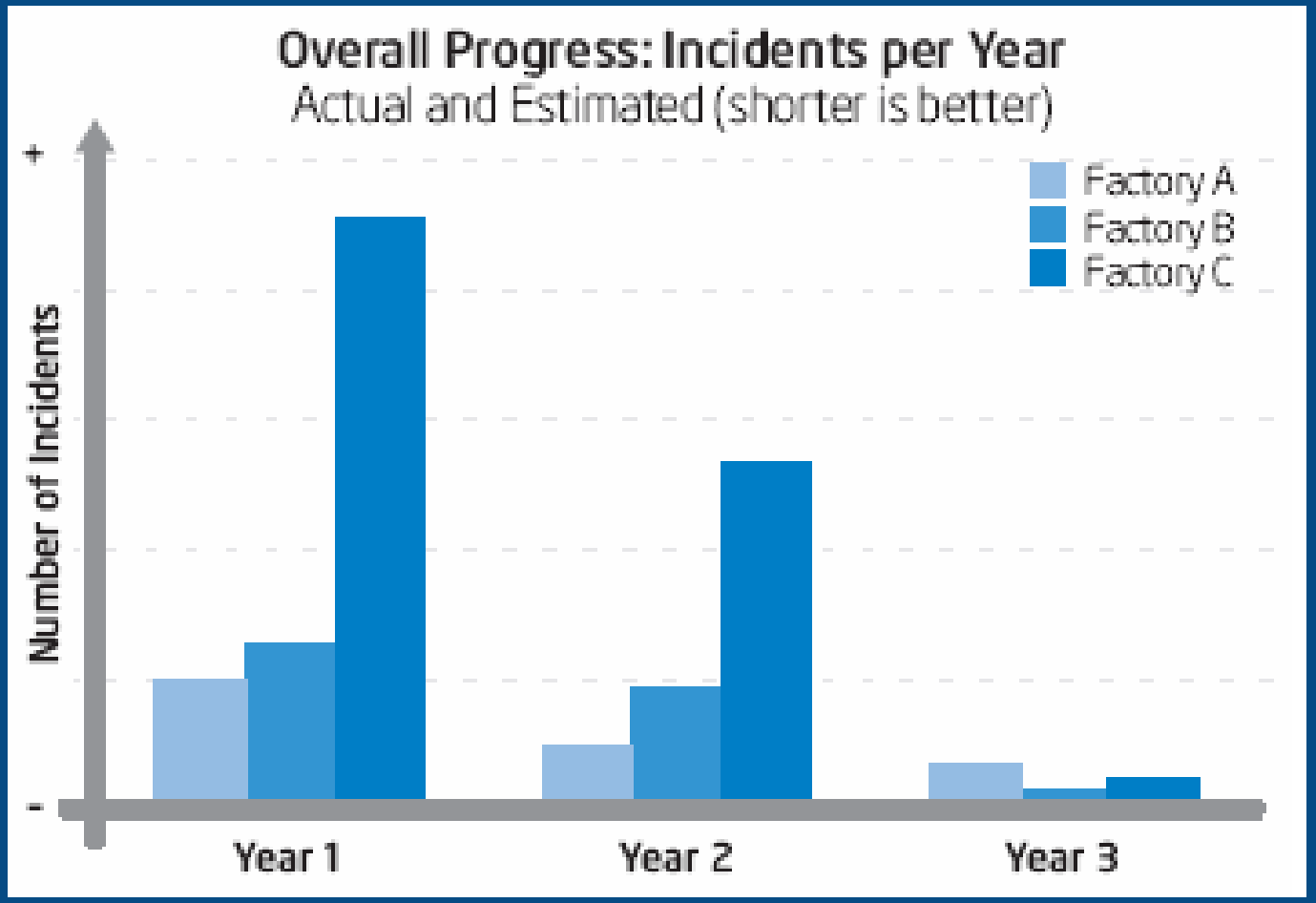
Assumptions

- Many factors, known and unknown, drive incident numbers
- Targeting accuracy sufficient to make good business decisions
- Only tracked the data for major security programs and ignored the minor changes
- Purposely conservative in assessing loss and value
- Assumed a relationship between the security controls and the number and frequency of incidents

Results


Overall Effects of Security Program
on Incident Occurrences
Baseline
Program A
Program B
Program C
Forecasted Incidents
Data Confidence

Results


Overall Progress: Incidents per Year
Actual and Estimated (shorter is better)
Factory A
Factory B
Factory C
Number of Incidents
+
-
Year 1
Year 2
Year 3

Results

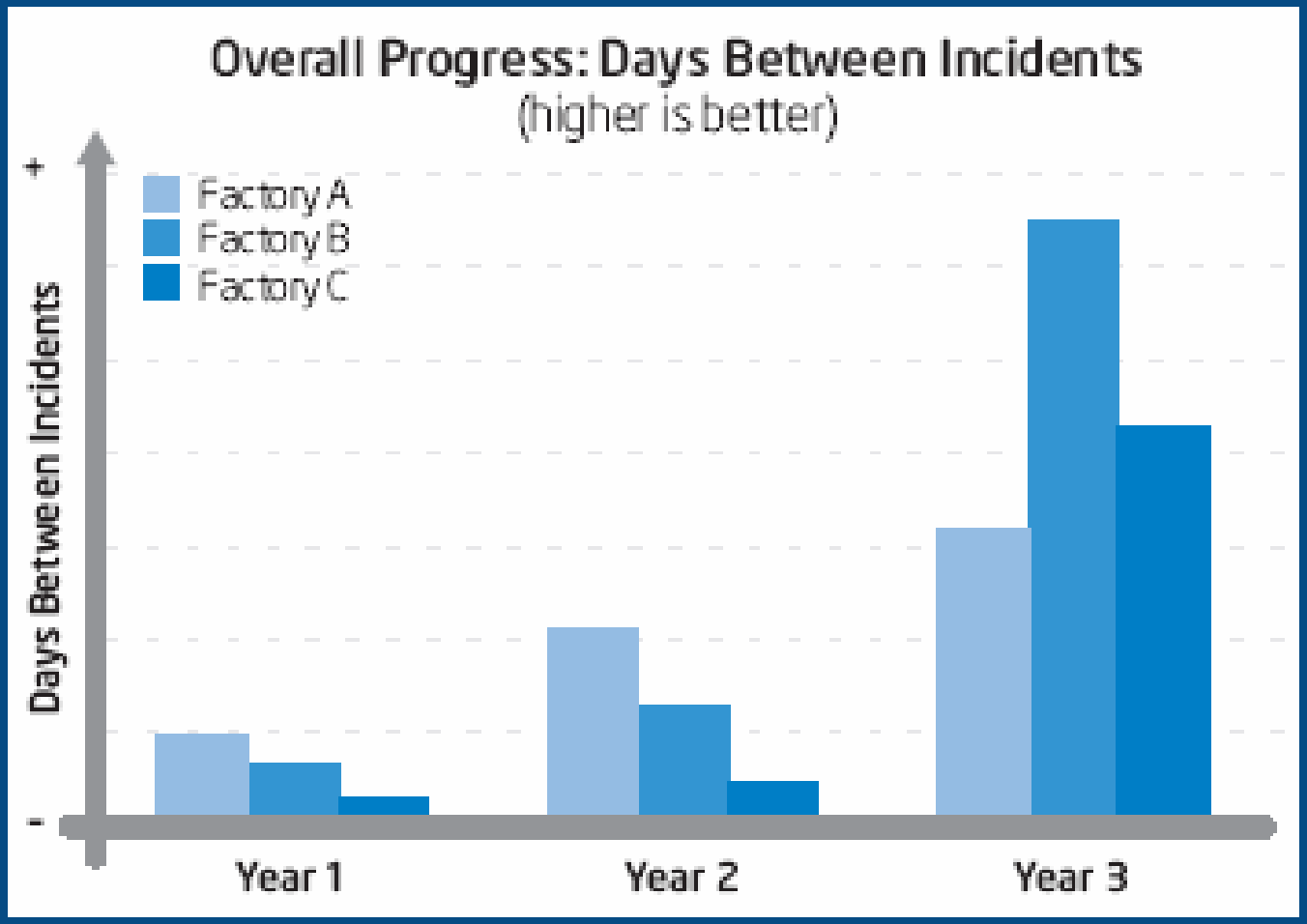
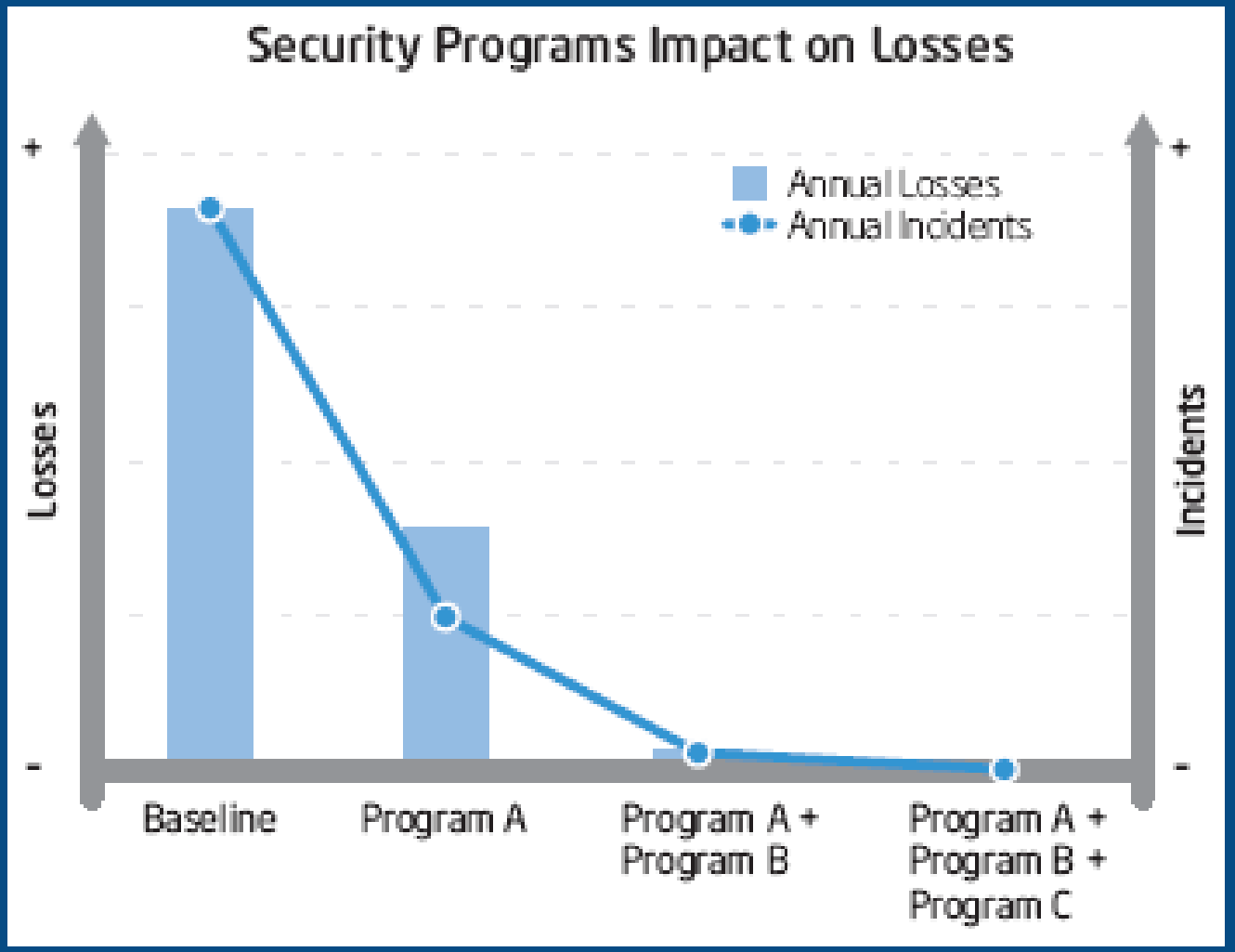


Figure 5. The combination of security programs

Results


Security Programs Impact on Losses
+
-
Losses
+
-
Incidents
Annual Losses
Annual Incidents
Baseline
Program A
Program A + Program B
Program A + Program B + Program C

Results

Efficiency of Security Programs Based on Avoided Incidents.

Security Programs	Incident Reduction
Program A	74%
Program B	91%
Program C	89%
Program A + B	97%
Program A + B + C	99%

Forecast of Predicted Incidents and Loss

Security Programs	Incident Reduction	Days Between Incidents Increase
No Security Programs	—	—
Program A	74%	4x
Program A + B	97%	45x
Program A + B + C	99%	396x

In Conclusion

Model is straightforward scientific method (nothing innovative, just taking a step forward)

Seeks a level of accuracy necessary to make good business decisions

Requires lots of data and test environments, but returns are impressive

Not a 'silver bullet'. Only applicable to specific situations

Tough to argue with the accuracy

- 5 months 94% accurate (incident prediction)
- 12 months 87% accurate (incident prediction)


intel®
Leap ahead™